WILLKIE FARR & GALLAGHER LLP
BENEDICT Y. HUR (SBN: 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN: 246943)
sagnolucci@willkie.com
EDUARDO E. SANTACANA (SBN: 281668)
esantacana@willkie.com
ARGEMIRA FLÓREZ (SBN: 331153)
aflorez@willkie.com
HARRIS MATEEN (SBN: 335593)
hmateen@willkie.com
333 Bush Street, 34th Floor
San Francisco, CA 94104
Telephone: (415) 858-7400

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ANIBAL RODRIGUEZ, *et al*. individually and on behalf of all others similarly situated,

Plaintiff,

vs.

GOOGLE LLC, *et al*.,

Defendant.

Case No. 3:20-CV-04688 RS

NOTICE OF ERRATA FOR GOOGLE LLC'S MOTION FOR SUMMARY JUDGMENT (DKT. 381)

(CIVIL LOCAL RULE 79-5)

Date: July 25, 2024
Time: 1:30 p.m.
Courtroom: 3, 17th Floor
Judge: Hon. Richard Seeborg

Action Filed: July 14, 2020
Trial Date: February 10, 2025

NOTICE OF ERRATA

Defendant Google LLC respectfully submits this errata in order to correct inadvertent clerical errors in Google LLC's Motion for Summary Judgment, filed on March 28, 2024 as Docket No. 381. The revisions (1) correct typographical errors to certain citations to the record or citation style errors and (2) update the Motion's hearing date to reflect the Court's availability.

The revised Motion is attached hereto as **Exhibit 1** and the "redline" demonstrating revisions to Docket No. 381 is attached as **Exhibit 2**.

Dated: April 4, 2024

WILLKIE FARR & GALLAGHER LLP

By: */s/ Eduardo E. Santacana*
Eduardo E. Santacana
Benedict Y. Hur
Simona A. Agnolucci
Argemira Flórez
Harris Mateen

Attorneys for Defendant
GOOGLE LLC

EXHIBIT 1

WILLKIE FARR & GALLAGHER LLP
BENEDICT Y. HUR (SBN: 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN: 246943)
sagnolucci@willkie.com
EDUARDO E. SANTACANA (SBN: 281668)
esantacana@willkie.com
ARGEMIRA FLÓREZ (SBN: 331153)
aflorez@willkie.com
HARRIS MATEEN (SBN: 335593)
hmateen@willkie.com
333 Bush Street, 34th Floor
San Francisco, CA 94104
Telephone: (415) 858-7400

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ANIBAL RODRIGUEZ, *et al*. individually and on behalf of all others similarly situated,

Plaintiff,

vs.

GOOGLE LLC, *et al*.,

Defendant.

Case No. 3:20-CV-04688 RS

GOOGLE LLC'S MOTION FOR SUMMARY JUDGMENT

Date: July 25, 2024
Time: 1:30 p.m.
Courtroom: 3, 17th Floor
Judge: Hon. Richard Seeborg

Action Filed: July 14, 2020
Trial Date: February 10, 2025

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

I. INTRODUCTION

This case started with Plaintiffs' allegation that data generated when users had turned off their Web & App Activity settings "is combined by Google into a user profile with all the other detailed, user-specific data Google collects on individuals and their devices," which "Google then uses [] to help generate billions of dollars in advertising revenues without users' consent." Compl., ECF No. 1[1], at ¶¶ 37–39,141–143, 146. None of that was true. Four years, hundreds of thousands of pages of produced documents, and almost 200 hours of fact and expert deposition testimony later, Plaintiffs have failed to produce a single shred of evidence substantiating that allegation. So, out of the ashes of their original theory, Plaintiffs seek to resurrect their case with the claim that Google should not have kept non-identifiable receipts for the ads it serves. And, the tortured theory goes, had Google not kept those receipts, advertisers would have refused to pay for advertising, so all of Google's advertising profit for ads served to WAA-off users should be forfeited. On that basis, Plaintiffs seek to convert their picayune liability theory into a half-billion dollar demand for class-wide judgment.

Since the allegations of Plaintiffs' current, certified theory—that Google promised not to engage in record-keeping, that Plaintiffs had a reasonable expectation the record-keeping would not occur, and that Plaintiffs suffered harm as a result of the record-keeping—are completely lacking in factual basis, the Court should grant summary judgment and dismiss this case with prejudice.

First, Google repeatedly disclosed and secured the consent for its basic record-keeping practices, which involve logging "non-personal information" for the purpose of reporting how ads and mobile apps are performing.

Second, each Plaintiff saw these disclosures, but argues that the WAA webpage led them to believe they could disable Google's record-keeping by switching WAA to "off." But the WAA webpage describes the button as a way to give or withhold permission for Google to "save" app activity data "to your Google Account" for the purpose of "personaliz[ing]" the user's experience. There is no reasonable interpretation of this language, in isolation or in concert with the Privacy

[1] Google will submit a hard-copy courtesy booklet of selected docket entries that are not listed in Appendix A (Evidentiary Material) or Appendix B (Previously Filed Under Seal Material) for the Court's ease of reference.

Policy, that extends the ambit of the WAA control to Google's non-personal record-keeping. And to the extent it was not immediately obvious from the WAA webpage that "to your Google Account" limited the ambit of the control, the Privacy Policy, which each Plaintiff alleges they reviewed, repeatedly explained that Google distinguishes between personally identifiable information and non-personal information.[2] The information Google used to keep its records was non-personal information, and Google used it in the precise ways it told Plaintiffs it would.

Third, Google did *not* use the information at issue to target or personalize ads, or build marketing profiles of WAA-off users. Plaintiffs originally alleged Google did so, but they never had a basis to make this allegation, and they abandoned that theory at class certification.

Finally, Google's basic record-keeping doesn't hurt anyone. Logging the fact that Google has served an ad to a randomly generated identifier that is never linked to a Google user's identity cannot be said to have exploited any class member's privacy, nor intruded upon their private space, nor taken from them anything they intended to keep for themselves or sell to another.

Nor can Plaintiffs fall back on disgorgement of profits as a basis to establish Article III or statutory standing, nor harm for their privacy torts. While the Ninth Circuit had, in a single sentence, ruled that such claimants can establish Article III standing in *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020), that is no longer good law in the wake of *TransUnion. See TransUnion LLC v. Ramirez*, 594 U.S. 413, 424–25 (2021). Nor did the Ninth Circuit purport to rule on the question of statutory standing or the element of harm required for privacy torts.[3]

---

[2] *See* Declaration of Anibal Rodriguez in Support of Class Certification, ECF No. 315-7, at ¶ 3 (Appx. A-5) ("When I opened my Google account in 2014, and in the years before filing this lawsuit, I had read Google's Terms of Service, Privacy Policy, and other Google disclosures to understand what data was and was not collected when WAA and sWAA were turned off. I agreed to those terms."); Decl. of Sal Cataldo, ECF No. 315-5, at ¶ 3 (Appx. A-3) (same); Decl. of Julian Santiago, ECF No. 315-8 (Appx. A-6) (same); Decl. of Susan Harvey, ECF No. 315-6, at ¶ 3 (Appx. A-4) (same).

[3] *See McClung v. AddShopper, Inc.*, No. 23-cv-01996-VC, 2024 WL 189006, at *2 (N.D. Cal. Jan. 17, 2024) ("The Court continues to be skeptical of the plaintiffs' theory that California's statutory standing requirement for these claims can be satisfied simply by alleging that the defendant was unjustly enriched by the misappropriation of personal information . . ." and "[T]he Article III analysis in that section of *Facebook Internet Tracking* has been superseded by *TransUnion*, making it even more of a stretch to rely on that section as an implicit statement about statutory standing under California law.") (citing *TransUnion*, 594 U.S. at 426–30); *see also id.* (citing *Hazel v. Prudential Financial, Inc.*, No. 22-cv-07465-CRB, 2023 WL 3933073, at *6 (N.D. Cal. June 9, 2023) ("Just because Plaintiffs' data is valuable in the abstract, and because [a company] might have made money from it, does not mean that Plaintiffs have 'lost money or property' as a result.").

II. PROCEDURAL BACKGROUND

A. Plaintiffs' original Complaint and Google's Motions to Dismiss

Plaintiffs filed their original complaint against Google LLC and Alphabet Inc. in July 2020, asserting claims for violation of the Federal Wiretap Act, section 631 (wiretap) and 632 (eavesdropping) of the California Invasion of Privacy Act ("CIPA"), invasion of privacy, and violation of the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502 *et seq.* ECF No. 1.[4] Google moved to dismiss in October 2020, ECF No. 48, and Plaintiffs amended their complaint rather than oppose, (First Am. Compl. ("FAC")), ECF No. 60. The FAC added several Plaintiffs, many of whom have since voluntarily withdrawn from the case.[5] The FAC also asserted two more causes of action for violation of the California Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq.* and for common law intrusion upon seclusion.

Google moved to dismiss every claim in the FAC. ECF No. 62. This Court ruled on that motion on May 21, 2021, granting the motion with leave to amend as to Plaintiffs' claims for violation of the Federal Wiretap Act, section 632 of CIPA, and the Unfair Competition Law. ECF No. 109, at 17–18. Applying Rule 9(b), the Court also dismissed Plaintiffs' theory of the case as to purported "secret scripts" embedded in Google's Android mobile operating system that supposedly facilitated unlawful interceptions of communications, again with leave to amend. *Id.* at 11–12.

Plaintiffs' Second Amended Complaint ("SAC") dropped the Federal Wiretap Act and Unfair Competition Law claims, and disavowed the "secret scripts" theory, but added a breach of contract claim. ECF No. 113, at 68–71. Google moved to dismiss again, this time only as to Plaintiffs' claims for breach of contract and violation of section 631 of CIPA. ECF No. 115. This Court granted Google's motion as to both claims, holding that Plaintiffs failed to state a claim for relief as to breach of contract, and that Plaintiffs' allegations established that Google's alleged wrongful use of recorded communications between users and app developers took the alleged conduct outside the ambit of CIPA section 631, since that statute requires simultaneous wiretapping

[4] All references to "ECF" are for docket entries in the above-captioned matter. Google also provides cited ECF entries to the Court in its "Courtesy Copy of Selection of Docket Entries."

[5] The withdrawn Plaintiffs are: Eliza Cambay, Emir Goenaga, JulieAnna Muniz, Julian Santiago, Harold Nyanjom, and Kellie Nyanjom.

for liability. ECF No. 127. In their SAC, Plaintiffs also added factual allegations concerning the integration of Google Analytics for Firebase with AdMob and with Firebase Cloud Messaging. This Court ruled those allegations could stand because Plaintiffs put Google on notice of their allegations that Google Analytics for Firebase and those two products are integrated such that the latter products use data collected by the former. *Id.* at 3, 7–8.

Plaintiffs filed their Third Amended Complaint ("TAC") on September 1, 2021, re-asserting their breach of contract and CIPA section 631 claims. ECF No. 131 (unredacted at ECF No. 130). Google moved to dismiss those claims again, ECF No. 139, and the Court dismissed them with prejudice. ECF No. 209. Google answered the TAC on February 22, 2022. ECF No. 230.

Finally, in late 2022, two days before discovery closed, Plaintiffs sought to amend their complaint again to add Google Search as an accused product in the case. ECF No. 258. This Court denied that motion for leave to amend while permitting an unopposed amendment to the extant class definitions. ECF No. 281. The operative Fourth Amended Complaint ("4AC") was filed on January 4, 2023. ECF No. 289.

B. Plaintiffs' theory of liability on the pleadings

Through successive orders on Google's motions to dismiss, this Court narrowed Plaintiffs' case to a simple and straightforward claim. As described by the Court in its first Order on Google's Motion to Dismiss the FAC, Plaintiffs allege that Google Analytics ("GA") for Firebase, a tool Google provides to app developers for use on mobile devices, "when functioning as advertised in a given app, contravenes [Google's] user-facing privacy representations." ECF No. 109, at 1. If, as Plaintiffs allege, GA for Firebase ("GA4F") does contravene Google's user-facing privacy representations, this Court ruled, Plaintiffs would have claims against Google for violation of the CDAFA and the common law torts of intrusion upon seclusion and invasion of privacy. *Id.* at 14–16.

In particular, Google makes available to users "a complex user-facing privacy apparatus" for controlling various privacy-related aspects of the user experience. *Id.* at 2–4. One such tool is an account setting (among others) called "Web & App Activity," or WAA. The WAA button[6] "purports

[6] Following the Court's May 2021 Order Granting in Part Google's Motion to Dismiss, Plaintiffs amended

to give consumers control over a defined subset of Google's data-gathering efforts." *Id.* at 3. Specifically, it tells users that if they turn on the toggle, that will "let Google save" certain information to "an individual's 'Google Account.'" *Id.* at 3. That set of data comprises "'info about [the individual's] searches and other activity on Google sites, apps, and services,' as well as 'info about [the individual's] . . . activity on sites, apps, and devices that use Google services.'" *Id.* The Court found particularly relevant in these disclosures two undefined terms—"Google services" and "Google Account." Depending on how a user interprets those terms, this Court held, a reasonable user could potentially be misled by the description of the WAA button in light of how GA4F works. *Id.* at 8–10.

GA4F is an enterprise-facing product that app developers can use for free. *Id.* at 4. When functioning as advertised, "GA for Firebase will automatically send various interactions between the app and its users . . . to Google, which will then present a clean, optimization-minded analysis of that data to the developer." *Id.* at 4. To use GA4F, app developers must agree to obtain consent for end users for the developer's use of GA4F. *Id.* at 4–5 & n. 3 (discussing "GA for Firebase Materials," a "suite of agreements, policies, and resources" provided to developers in Google's publicly-available online "Help Center"). As described by the Court, Plaintiffs allege that GA4F contravenes the WAA description as follows:

> Plaintiffs allege Google's capture and analysis of data via GA for Firebase, on behalf of app developers who knowingly utilize that service, violates the WAA Materials' representations to individuals who have disabled the WAA feature. Under this theory of liability, GA for Firebase—when running as marketed—allows Google to collect information about an individual's "activity on . . . apps . . . that use Google services," notwithstanding the WAA Materials' statement that "[t]o let Google save this information . . . Web & App Activity *must* be on."

Id. at 6 (emphasis in original). Further, this Court ruled that the phrase "Google Account" was sufficiently ambiguous that a user could reasonably believe that turning WAA off would prevent

their complaint to include descriptions of the supplemental Web & App Activity ("(s)WAA") button. *See* 4AC, ECF No. 289. The (s)WAA button provides users with the option to allow Google to save "Chrome history and activity from sites, apps, and devices that use Google services" to the user's Google Account. *Id.* at 22. WAA must be on for (s)WAA to be on. *Id.* Thus, when a user disables the WAA toggle, the (s)WAA button is also disabled. *Id.* In this case, the parties refer to the two controls collectively as "WAA" or "(s)WAA".

Google from saving GA4F data linked to that user's "e-mail address," or that "monitors" that user's activity across the web, or that personalizes that user's experiences across Google services. *Id.* at 8–9. As a result, Plaintiffs stated a claim for violation of the CDAFA because Google's data collection was allegedly "without permission," and for invasion of privacy because the question of whether the user consented and whether the collection was highly offensive were inappropriate for resolution on the pleadings. *Id.* at 14–16. Those are the claims that have survived through later motions to dismiss. As of today, four named Plaintiffs remain: Sal Cataldo, Susan Lynn Harvey, Anibal Rodriguez, and Julian Santiago. *See* 4AC, ECF No. 289.

C. The discovery period

In total, the parties engaged in 48 months of fact discovery and 5 months of expert discovery, comprising 211,186 pages of produced documents, 1,113 pages of expert reports, 2,201 pages of expert depositions, and 4,239 pages of witness deposition transcripts. Santacana Decl. ¶ 3. When necessary, the parties appealed to Judge Tse to resolve discovery disputes. In all, Judge Tse issued 21 Orders resolving 25 discovery disputes. Santacana Decl. ¶ 3. At the close of fact discovery, Plaintiffs requested a two-month extension of the discovery period on the grounds that Google had engaged in alleged discovery misconduct. ECF No. 279. This Court denied that motion in December 2022. ECF No. 282.

D. The Court's Order granting Class Certification

Following expert discovery, Plaintiffs moved for class certification, ECF No. 315, and Google opposed, ECF No. 329. The Court issued its Order granting class certification on January 3, 2024, ECF No. 352, certifying two classes of plaintiffs comprising individuals who turned off (s)WAA and used Firebase – or Google Mobile Ads – enabled apps.

In order to secure class certification, Plaintiffs disclaimed a variety of arguments and pressed to the Court the theory that the mere collection of app activity data, absent any use by Google, and even if it is made pseudonymous or anonymous, nevertheless contravened Google's description of the WAA button, and that the difference could be used to hold Google liable class-wide.

Accepting Plaintiffs' arguments, the Court granted class certification and rejected Google's arguments concerning individualized issues. *Id.* In particular, the Court reasoned that Google's

consent defense could be decided class-wide because "Google's representations about the WAA feature, unambiguous and persistent by its own admission, outweigh these individual questions about *where* class members learned about the WAA feature." *Id.* at 15–16 (emphasis in original). Further, the Court held that "the relevant 'conduct' showing a lack of consent is the users' decisions affirmatively to switch off the WAA and sWAA buttons," which this Court held constituted a "common act representing their privacy choices, based on Google's own ubiquitous representations." *Id.* at 9–10. In addition, the Court held that "even if Google is right, and the 'vast majority' of class members' data was only exposed to record-keeping 'not tied to a person's identity or used by Google for any purpose other than to perform accounting for the apps that generated the data or advertising in the first place,' Opp. at 16, then surely that can be proven by common evidence of Google's record-keeping practices." *Id.* at 12.

III. STATEMENT OF FACTS

The following statement of facts is undisputed. To the extent Plaintiffs dispute any fact below, Google respectfully submits that no evidence in the record supports such a position.

A. Plaintiffs concede that Google does not personalize advertising with (s)WAA-off data; the certified theory of liability challenges basic, pseudonymous record-keeping.

GA4F is "an app measurement solution" used by mobile app developers for "insight on app usage and user engagement." *See Google Analytics*, Firebase, ECF No. 324-1(Appx. A-8).[7] Using GA4F, app developers can measure various "events," or specific types of user interactions with their apps.[8] *See* Expert Report of Jonathan Hochman ("Hochman Rpt.,") ECF No. 361-58, ¶¶ 89–91 (Appx. A-11); Interrog. Set One Resps., ECF No. 364-1, at 4:20–5:6 (Appx. A-13). As a service provider, Google accepts bundles of event data from app developers' apps and stores and analyzes them for those developers regardless of a user's (s)WAA setting. ECF No. 364-1, at 10:15–11:5, 28:4–28:23 (Appx. A-13).

[7] *See also* Interrog. Set One Resps., ECF No. 364-1, at 5:8–21; "App Attribution in GAA," ECF No. 364-2, at -515 (Appx. A-14) (Unsealed Version at Appx B-4); Hochman Rpt., ECF No. 361-58, at ¶ 62 (Appx. A-11).

[8] Default events include, for example, the first opening of an app, or when a user clicks on a certain part of the app. ECF No. 361-58, ¶ 94 & n. 84; Interrog. Set One Resps., ECF No. 364-1, at 4:20–5:21 (Appx. A-13); *see also* ECF No. 324-4 (excerpting "[GA4] Automatically collected events") (Appx. A-9).

As long as they comply with Google's terms of use, app developers can also customize their usage of GA4F. *See* Historic GA4F Terms of Service (Appx. A-2); ECF No. 65, at 5–6 (Appx. A-1).[9] Per Google's terms, apps must disclose and obtain consent from end users to use the SDK. *Id.*

In their complaints, Plaintiffs alleged that Google saves WAA-off data to marketing profiles and uses them to personalize advertising, that Google "includes in its user profiles" data "secretly transmitted to Google" by "tracking and advertising code," *i.e.* GA4F. And they claimed that by "including this data in its user profiles, Google increases the user profiles' value" and "allows Google to more effectively target advertisements to these users"; and that "this [sWAA-off] data is combined by Google into a user profile with all the other detailed, user-specific data Google collects on individuals and their devices," which "Google then uses [] to help generate billions of dollars in advertising revenues without users' consent." ECF No. 1, ¶¶ 37–39, 141–143, 146.

Over the course of this lawsuit, Plaintiffs' narrative shifted; they and their experts now concede these allegations were false.[10] Indeed, Google's verified interrogatory response, served nearly three years ago, made it clear: **Google does not save WAA-off data to any Google user's marketing profile, and does not use WAA-off data for personalized advertising, either in connection with a user's true identity *or* in connection with a user's pseudonymous identity.**[11] Interrog. Set One Resps., ECF No. 364-1, at 7:7–14 (Appx. A-13). Plaintiffs no longer contend, as they once did, that Google secretly collects (s)WAA-off data to create profiles for personalized advertising. Instead, Plaintiffs argue that Google uses (s)WAA-off data for basic record-keeping. And, in their Motion for Class Certification, Plaintiffs paradoxically argued that Google conceals its basic record-keeping with (s)WAA-off data "by turning off 'personalized' ads that could tip [users] off to Google's continued tracking." Class Cert. Mot., ECF No. 361-1, at 2. That is, for most

[9] *See also* Additional Historic GA4F Terms of Service, (Appx A-2).

[10] *See* Dep. Tr. of Jonathan Hochman ("Hochman Tr."), ECF No. 364-19, at 194:18–24 (Appx. A-20) (Q. "[Y]ou're not disputing in this case that Google will not personalize ads . . . with sWAA-off Google analytics for Firebase data?" A. "That's correct."). *See also* Dep. Transcript of Michael Lasinski ("Lasinski Tr."), ECF No. 364-17, at 79:16–18 (Appx. A-19) ("[M]y understanding is that Google has represented that sWAA-off users do not receive personalized ads."); *id.* at 81:6–9 (Q. "So for neither scenario did you assume that sWAA-off users were receiving personalized ads that relied on sWAA-off data?" A. "Correct.").

[11] *See also* Google's Resps. to Plaintiffs' Interrog., Set Six, ECF No. 364-22, at 8:21–10:9 (Appx. A-22); Interrog. Set One Resps., ECF No. 364-1, at 23:15–25:23 (Appx. A-13); Interrog. No. 18 Resps., ECF No. 364-8, at 5–6; Dep. Tr. of Belinda Langner ("Langner Tr."), ECF No. 364-7, at 78:2–7 (Appx. A-18).

of the pendency of this case, Plaintiffs maintained that Google's alleged personalization of advertising with (s)WAA-off data was deceptive; now they argue that Google's decision not to personalize advertising with (s)WAA-off data is deceptive.

Specifically, the Motion argued that Google contravenes its representations because, even when a user's (s)WAA is turned off, Google will still (1) log the fact that it has served an ad alongside a device identifier for accounting purposes, and (2) attribute conversion events to those ad serving records. *See* ECF No. 361-1, at 14. Plaintiffs' damages theory relied upon to obtain class certification focuses on this use of (s)WAA-off data, positing that (1) "[i]f Google did not collect and save ad requests, it could not serve ads. And without data regarding both ad requests and the ads that Google served, Google would lack the records it needs to charge advertisers for its services" and (2) "Google also uses this ads data to track conversions; if it lacked data regarding a user's interaction with an ad, it would be unable to determine whether that interaction is related to any later behavior." Hochman Rpt., ECF No. 361-58, ¶ 122 (Appx. A-11).[12] The logging of the (s)WAA-off record of ad service or analytics conversion events is, in Plaintiffs' view, an indispensable link in a long chain that ends in advertisers paying for advertising.[13] Thus, Plaintiffs claim, Google should be disgorged of *all* profit made from serving any ads to (s)WAA-off users on mobile apps, because to perform the serving of the ad, Google had to exchange information with the mobile app where the ad was served, and keep a record that it served it. *Id.* at ¶ 271; Lasinski Tr., ECF No. 364-17, at 129:12–18 (Appx. A-19).

At a technical level, the practice Plaintiffs complain of as profit-making is the use of

[12] *See id.* ¶ 271 ("[B]ut for Google's collection of WAA-off or sWAA-off data, Google would not be able to serve advertisements to those users and then charge the advertisers because Google would lack the necessary data records to back up their advertising charges."); Lasinski Tr, ECF No. 364–17, 113:1–3, 113:20–23 (Appx. A-19) ("The advertiser would pay less to Google because Google did not – would not serve an ad in those cases. . . . [T]hey would pay them less because those ads that are currently being shown to sWAA-off users would not be shown to sWAA-off users."); *id.* at 137:8–14 ("My understanding is, based on input given to me, is that Google would not be able to serve an ad in those situations. Whether or not you want to call it an ad blocker, I've never called it that, but Google would not be able to serve an ad in those situations.").

[13] Plaintiffs have also complained that Google uses the (s)WAA-off data to improve Google's products and services (Class Cert. Mot., ECF No. 361-1, at 3), and engage in fraud and spam detection (Hochman Tr., ECF No. 364-19, at 204:25–209:10 (Appx. A-20)), but they do not assign these uses any value in their damages models and do not rely on these arguments to demonstrate class-wide injury.

(s)WAA-off records by Google to perform "attribution"[14] for advertisers. *See* Hochman Rpt., ECF No. 361-58, ¶¶ 279–296 (describing generally "Attribution/Conversion Tracking"); Appendix E to Hochman Report: Ad Campaigns and Conversion Tracking/Modeling (Appx. A-11); ECF No. 361-59, ¶¶ 12–26 (Appx. A-12) (Unredacted at Appx. B-1). Attribution can be performed in a number of ways. The specific technique Plaintiffs complain of works as follows:

1. **At Time 1**, an ad for the New York Times (NYT) app appears in the Nike app, which uses the Google Mobile Ads SDK (AdMob) to serve ads. An unidentified user clicks on it, causing the SDK to **log that the user's device ID clicked on that ad**.
2. Then, the user installs and opens the advertised NYT app. The NYT app uses the Firebase SDK and GA4F. As a result, **at Time 2**, the NYT app uses GA4F to **log that the user's device ID triggered the "first_open" analytics event**.
3. Google's ad system connects the dots on the back end: the same device ID that clicked on the ad at Time 1 triggered the "first_open" event at Time 2. If the two times are within a time period set by the advertiser (for example, 7 days), Google reports to the app developer/advertiser that **a conversion has occurred**. Over time, the app developer/advertiser receives aggregate reporting on the conversions they've achieved.

Measuring conversions varies from app to app because app developers can choose to rely on Google's default conversion events, like "first_open," or they can create their own custom conversion events.[15] Hochman Rpt., ECF No. 361-58 at ¶ 94 & n.84 (Appx A-11); *see also* "Log Events," Google Analytics (Appx. A-23). Plaintiffs have never offered any explanation for how this basic record-keeping activity harms users.

The conversion and ads logs in question are streamlined to contain just the critical pieces of information—which device triggered the event, the name of the event, which app sent Google the information, and other similar pieces of information. *See* Expert Report of John Black ("Black Rpt."), ECF No. 364-20, ¶ 92 (Appx. A-21); *see also* Hochman Rpt, App'x E, ECF No. 361-59 (Appx. A-12). So, for example, while a conversion event could be called "in_app_purchase," and it could contain for the app developer pseudonymous information about what the device purchased, for Google's attribution purposes, it is just the fact that the event occurred that is logged and later

[14] *See generally* "Attribution (Marketing)," Wikipedia, The Free Encyclopedia (last modified February 10, 2024), https://en.wikipedia.org/wiki/Attribution_(marketing).

[15] *See generally* "[GA4] Create or Modify Conversion Events," Google Analytics Help, accessed March 21, 2024, https://support.google.com/analytics/answer/12844695?hl=en

used to connect an ad click at Time 1 with a purchase at Time 2. *See* Black Rpt., ECF No. 364-20, ¶ 92 (Appx. A-21); *see also* Hochman Rpt., ECF No. 361-58, ¶¶ 122–123.

This accounting function is the basis for the certified theory of liability.

B. Google represented that the WAA button controlled whether data would be "saved to your Google Account," *i.e.*, "associated with your personal information."

The theory of liability certified by this Court centers around Google's representation that turning WAA[16] on would enable Google to "save" a user's activity data "in your Google Account." 4AC, ECF No. 289, at 27. Plaintiffs reason that the opposite should hold true as well; that is, if a user turns off WAA, that should disable Google from saving a user's activity data to that user's Google Account. As discussed below, that is exactly how WAA works.

Part of Plaintiffs' theory of liability rests on the term "**your Google Account**." This is a defined term. *See* Privacy Policies, ECF No. 323-1, at 52 (Appx. A-7). The Privacy Policy ("PP") has, since the start of the class period, explained that Google treats information "associated with your Google Account" as "personal information," which is distinct from "non-personally identifiable information." Privacy Policies, ECF No. 323-1, at 5, 52 (Appx. A-7). First, the PP explained that "Information we collect when you are signed in to Google, in addition to information we obtain about you from partners, may be associated with your Google Account. **When information is associated with your Google Account, we treat it as personal information.** For more information about how you can access, manage or delete information that is associated with your Google Account, visit the Transparency and choice section of this policy." *Id*. at 5; *see also id*. at 6–7, 11 ("Depending on your account settings, your activity on other sites and apps may be **associated with your personal information**" and Google "may share non-personally identifiable information publicly and with our partners").

Throughout the class period, the PP directed users to a "Key Terms" section if there were phrases they did not understand: "We've tried to keep it as simple as possible, but if you're not

[16] The (s)WAA control can only be enabled if WAA is also enabled.

familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first." *Id*. at 1. The Key Terms section in turn defined throughout the class period the phrases "Google Account," "personal information," and "non-personally identifiable information." *Id*. at 52. "**Google Account**" was defined as the Account a user signs up for by "providing us with some personal information" which can be used "to authenticate you when you access Google services; "**personal information**" was defined as information "which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google, **such as information we associate with your Google account**"; and "**non-personally identifiable information**" was defined as "information that is recorded about users so that it no longer reflects or references an individually identifiable user." *Id.* No section of the PP or the WAA page itself suggests to users that there is an account control to disable Google's collection or use of "non-personally identifiable information."[17]

C. Google's disclosures uniformly and unambiguously explained that it could use non-personal information for basic record-keeping.

Google discloses its uses of analytics and ads data in many contexts, and explains the difference between run-of-the-mill record-keeping using non-personal information and personalized advertising using personal information associated with a Google Account.

First, in its Privacy Policy, Google explained throughout the class period that Google uses "cookies or similar technologies to identify your browser or device" and to "collect and store information when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites," including "Google Analytics." ECF No. 323-1, at 4–5 (Appx. A-7). Further, the PP explained that analytics helps app owners "analyze the traffic to their [] apps" and "[w]hen used in conjunction with our advertising services . . . Google Analytics

[17] Further, since at least 2016, in a section linked from the PP called "How Google uses data when you use our partners' sites or apps," Google explained that "apps that partner with Google can send us information such as the name of the app and an identifier that helps us to determine which ads we've served to other apps on your device. If you are signed in to your Google Account, and depending on your Account settings, we may add that information to your Account, and treat it as personal information." ECF No. 323-1, at 54 (excerpting "How Google uses data when you use our partners' sites or apps" from Google's Privacy & Terms dated June 28, 2016 PP) (Appx. A-7). The account setting referenced here is, once again, the WAA setting.

information is linked, by the Google Analytics customer or by Google, using Google technology, with information about visits to multiple sites." *Id.* at 5.

The PP also explained that "we [Google] regularly **report to advertisers on whether we served their ad** to a page and **whether that ad was likely to be seen**." *Id.* at 23. Google's Privacy Portal also hosts a "How Ads Work" page, which again explained: "We give advertisers data about their ads' performance, but we do so without revealing any of your personal information." *Id.* at 29. Starting in March 2018, Google maintained a PP "Technologies" page, a corollary to the earlier "How Ads Work" page; that page again explained: "We store a record of the ads we serve in our logs"; "We anonymize this log data by removing part of the IP address (after 9 months) and cookie information (after 18 months)"; and "You can use Ads Settings to manage the Google ads you see and opt out of Ads Personalization," but "**[e]ven if you opt out of Ads Personalization, you may still see ads** based on factors such as your general location derived from your IP address, your browser type, and your search terms." *Id.* at 49.

Indeed, Plaintiff Sal Cataldo understood that (s)WAA was not an ad blocker and that while he could control ads personalization, he could not use (s)WAA or the ads personalization button to prevent Google from serving ads at all. Dep. Transcript of Sal Cataldo ("Cataldo Tr."), ECF No. 364–6, at 152:18–153:18 (Appx. A-17).

Plaintiffs have argued that the (s)WAA control should function as an ad blocker, and prevent Google even from keeping basic record-keeping of the ads it serves on behalf of third party advertisers. But there is no textual basis for this argument.

Throughout the class period, the PP explained that users can "[r]eview and update your Google activity controls to decide what types of data, such as videos you've watched on YouTube or past searches, you would like **saved with your account** when you use Google services." ECF No. 323-1, at 7 (Appx. A-7). The text of the WAA control explains: "The data ***saved in your account*** helps give you more ***personalized*** experiences across all Google services. Choose which settings will save data ***in your Google Account***." 4AC, ECF No. 289, at 27 (emphasis added).

Google repeatedly explained to users that they could affect the advertising Google serves to them via the "Ad Settings" button, ***not*** the WAA toggle. The PP and related disclosures made clear

that turning off the personalization setting would not prevent Google from serving ads, only make the ads less relevant. ECF No. 323-1, at 48–50 (Appx. A-7). In other words, Google disclosed that it would still perform its role as record-keeper for advertisers, and it would still serve ads, regardless of a user's Google Account Ad or WAA settings (and never represented that activity controls like WAA would have anything to do to the contrary).

D. Google never "saves to a user's Google Account," *i.e.*, personally identifies, (s)WAA-off Analytics or Ads data.

The WAA button says it can be used to give Google permission to save activity data to a user's Google Account. The button does exactly what it says it will do. When WAA is off, Google ***never*** saves activity data to a user's Google account. *See* Interrog. Set One Resps., ECF No. 364-1, at 11:19–13:17 (Appx. A-13); Interrog. Set Seven Resps, ECF No. 364-8, at 6:16–7:26; Hochman Rpt., ECF No. 361-58, at ¶ 205 & n.136 (Appx. A-11); Langner Tr., ECF No. 364-7, at 78:2–78:7 (Appx. A-18).

If the user's (s)WAA toggle—the toggle that applies to data from third-party apps—is set to "off," these data are ***never*** used by Google to identify users; they are processed and analyzed for the benefit of the app developer who generated the data, so they can better understand their own interactions with their own users and the success of their own advertising. Interrog. No. 1 Resps., ECF No. 364-1, at 16:19–17:5, 28:4–29:7 (Appx. A-13). Further, (s)WAA-off data is treated by Google strictly as pseudonymous data. *Id.*; *see* Dep. Transcript of Steve Ganem ("Ganem Tr.") ECF No. 364-3, at 44:16–19 (Appx. A-15). Google logs analytics and ads data alongside a randomly generated pseudonymous identifier (a device ID like ADID or IDFA on iOS) that is never mapped to the identity of the Google Account that was using the device. Interrog. No, 1 Resps., ECF No. 364-1, at 12:7–13:2 (Appx. A-13). Google never unmasks pseudonymous identifiers, and takes steps to ensure these pseudonyms are never re-unified to a user's identity. *Id.* at 8:2–9, 13:3–14:2, 23:15–25:23, 26:11–28:2; App'x X4 to Black Rpt., (sampling Google's "Anti-Fingerprinting" and User Data Access Policies) (Appx. A-16). The only circumstance in which Google saves *any* activity data to a user's Google account is when Google has first ensured the user has provided all required consents, including that (s)WAA is set to "on." Interrog. No. 1 Resps., ECF No. 364-1, at 23:15–

26:9 (Appx. A-13)

Plaintiffs do not contest any of this; indeed, when asked about this practice, Plaintiffs' technical expert conceded that Google "has the best intentions here" to keep pseudonymous and identifiable data separate, but complains that "maybe Google is nice today but they become evil in the future" and decides to re-unify data for a government or for profit.[18] Hochman Tr., ECF No. 364-19, at 364:18–365:5 (Appx. A-20).

E. Google has erected technical barriers to the joining of (s)WAA-off data with GAIA-keyed data.

Google takes significant steps to ensure that (s)WAA-off data are not re-associated with the user whose device generated the data. These steps vary from simple isolation of access to critical pieces of information to advanced cryptographic techniques that makes it a practical impossibility for anyone at Google or anyone else to be able to rejoin pseudonymous data to a user's identity.

First, when Google's servers perform a consent check to determine a user's (s)WAA setting, the device IDs are encrypted, and the server checking the user's consent status does not also receive the analytics data. *See* Interrog. No. 1 Resps., ECF No. 364-1, at 23:15–25:6, 26:11–28:2 (Appx. A-13). As a result, the physical machine that receives the encrypted device ID from user devices isn't able to decrypt it, and the physical machine that decrypts the device ID doesn't receive the measurement data. *Id.*

When a consent check returns a (s)WAA-off result, analytics data are logged to "pseudonymous space." *Id.* at 23:27–24:7, 25:7–8. These logs do not contain identifying information in them. For example, they do not contain GAIA IDs, which correspond to a user's Google Account identifier. *Id.* at 25:25–26:9. Likewise, GAIA-keyed logs in "GAIA space" at Google do not contain the identifiers in pseudonymous logs, such as device ID or unencrypted app_instance_id. *Id.* Further, for those pieces of information that overlap between the GAIA log and the pseudonymous log, they are encrypted differently and the decryption keys are thrown away after

[18] Even if there is a potential for rare instances of violation of Google's terms of service by app developers, that is *not* the basis of any certified theory of liability in this case, as any such idiosyncrasy could not be said to be uniform across the class, nor could Google be held liable for it, since causation would in that case depend on a third party's conduct.

six days, making it impossible to match up fields in one log to the other. *Id.* at 27:8–21.

Google limits access to these decryption keys to select individuals, and if any unauthorized individual seeks access to them, Google has systems in place that will prevent them from obtaining access. *See* Interrog. Set One Resps., ECF No. 364-1, at 27:15–28:2 (Appx. A-13); *see also* Black Rpt., ECF No. 364-20, at ¶¶ 171, 178 (Appx. A-21). Google also "salts" data in GAIA logs, meaning random data is added to it, to make it even harder to match it up to overlapping data sets in pseudonymous logs. ECF No. 364-1, at 26:7–9 (Appx. A-13).

Finally and most importantly, Google employees are flatly forbidden from performing a "join" of data that would unmask the identity of an individual whose data was logged in pseudonymous space. *Id.* at 24:9–15, 27:22–28:2.[19] Many of these controls have been in place since Google launched GA4F; others have been adopted over time. Google's prohibition on circumventing these privacy controls, however, have been in place at least since GA4F launched. *See* App'x X4 to Black Rpt. (compiling "Anti-Fingerprinting" Policies as far back as January 21, 2015) (Appx. A-16).

IV. UNDISPUTED MATERIAL FACTS

In light of the foregoing statement of facts, and for the ease and convenience of the Court, Google submits that the following undisputed material facts resolve this dispute in its entirety, understanding the Court may also find other undisputed facts described above material as well.

1. At all relevant times, Google represented that the WAA button controlled whether certain data would be "saved to your Google Account."

2. At all relevant times, the phrase "saved to your Google Account" limited the ambit of the WAA button to permissions relating to saving data in a manner that was associated with personal information.

3. At all relevant times, Google represented through its Privacy Policy and Privacy Portal that the phrase "saved to your Google Account" meant "associated with your personal information," not "saved" in any form, for any purpose, even if made pseudonymous.

[19] *See also* App'x X4 to Black Rpt., ECF No. 364-4 (Appx A-16) (compiling Google's "Anti-Fingerprinting" Policies); "GEO Privacy Champion", ECF No. 361-13, at - 411 (Appx. A-10); ECF No. 314-7, (Unsealed Version, Appx B at B-2); Ganem Tr., at 44:1-44:19, (Appx. A-15); Hochman Tr., ECF No. 364-19, at 135:25–136:1 (Appx. A-20) ("Yeah, I don't think I necessarily found an indication of joining.").

4. At all relevant times, Google's Privacy Policy defined "personal information" to mean information "which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google, such as information we associate with your Google account," or a substantially similar definition.

5. Google did not save the WAA-off or (s)WAA-off data at issue in this case generated by class members to that class member's Google Account.

6. Google did not associate the WAA-off or (s)WAA-off data at issue in this case generated by class members with the class members' personal information.

7. Google maintained the WAA-off or (s)WAA-off data at issue in this case generated by class members in pseudonymous or anonymous form in a manner that disabled Google employees from personally identifying the user that generated the data.

8. Google never used the WAA-off or (s)WAA-off data at issue in this case generated by class members to personalize advertising to class members or build marketing profiles.

V. ARGUMENT

Plaintiffs' case hinges on the factual claim that Google saved app activity data gathered by GA4F to Plaintiffs' Google Accounts while (s)WAA was switched off. Because Google represented that it would save such data to a user's Google Account only when they had turned WAA on, Plaintiffs argue, Google violated its promises to users and thereby their privacy rights. That same theory underlies the Court's decision to permit some of Plaintiffs' claims to proceed past the pleadings stage. ECF No. 109, at 3–4, 6. Per the Court, "[u]nder this theory of liability, GA4F—when running as marketed—allows Google to collect information about an individual's 'activity on . . . apps . . . that use Google services,' notwithstanding the WAA Materials' statement that '[t]o let Google save this information . . . Web & App Activity must be on.'" *Id.* at 6. (original emphasis and alterations).

And the same theory is what ultimately was certified by the Court for a class trial. ECF No. 352. In particular, the Court accepted Plaintiffs' argument that the only questions necessary to decide this case are (1) what Google represented, (2) what Google's uniform conduct was, and (3) whether any variance between them rises to the level of liability. *E.g., id.* at 11.

The answers to these three questions are straightforward. (1) Google represented that the WAA button would control whether Google had permission to save activity data to the user's

Google Account. (2) Google does not save activity data to the user's Google Account when (s)WAA is off. And (3) Google's practice of keeping basic, pseudonymous records of its advertising does not deviate from its representations concerning (s)WAA. Therefore, there is no liability under the CDAFA or Plaintiffs' invasion of privacy claims.

A. Plaintiffs consented.

Consent is an absolute defense to each of Plaintiffs' remaining claims: CDAFA, invasion of privacy, and constitutional invasion of privacy. Because no reasonable juror could find that Plaintiffs reasonably believed (s)WAA did what they claim, Google's consent defense alone requires a full dismissal of Plaintiffs' claims.

In granting class certification, this Court accepted Plaintiffs' argument that "express consent does not defeat predominance because the "'sWAA disclosures and Google's Privacy Policy' are the only relevant materials for analysis, and are 'the same for all class members.'" ECF No. 352, at 15 (quoting Plaintiffs' Class Cert. Reply, at 10). The Court held that Google's consent defense could be decided class-wide because "Google's representations about the WAA feature, unambiguous and persistent by its own admission, outweigh these individual questions about where class members learned about the WAA feature."[20] *Id.* at 15–16.

Now is the time to make that determination. Plaintiffs by their own argument invited an evaluation of these two sets of uniform representations. If these representations are unambiguous, or are not susceptible to Plaintiffs' reading of them, their case must end.

The representations are unambiguous. As discussed above, the description of (s)WAA was plain and straightforward: the button controls whether Google has permission to "save" "web & app activity data" to a user's "Google Account."[21] Google does not "save" "app activity data" sent to it via GA4F or the Google Ads products in question, or any product or service addressed by Plaintiffs,

[20] Google also argued that class members consented in various ways to Google's conduct by consenting to third party apps' privacy policies. This Court ruled that such consent was not relevant to Google's liability, which could be determined class-wide, because "the relevant question concerns Google's disclosures about the sWAA button, not third-party disclosures to users," and "[t]o the extent Google had a policy that required third party apps to disclose Google's policies to users, that evidence may be applied across the class." ECF No. 352, at 17. As such, these third party disclosures cannot now create a material issue of disputed fact.

[21] There is also a use limitation in how (s)WAA is described: that the permission is for using the data to "personalize experiences" across Google. Compl., ECF No. 1, at ¶ 49.

to a user's "Google Account." *See* Interrog. Set One Resps., ECF No. 364-1, at 23:27–24:7 (Appx. A-13). Instead, Google's uniform policy and practice is to take significant steps to separate (s)WAA off data from any personally identifiable information belonging to the end user who generated the data. *See id*. at 24:5–28:2, & App'x X4 to Black Rpt., (Appx. A-16).

To the extent any user was confused by the plain meaning of the (s)WAA representations, they were also uniformly presented with Google's Privacy Policy and Privacy Portal, which repeated the distinction between data saved to a "Google Account" and data that is not "associated with personal information" in numerous places. *See supra* III.B. (discussing historic representations made in Google's Privacy Policies, ECF No. 323-1 (Appx. A-7)).

There is no ambiguity to be exploited here. For four years, Plaintiffs have repeated their constant refrain that "off" means "off"; that (s)WAA was a light switch, and that whatever (s)WAA meant, turning it off should do the opposite of what turning it on does. There is no dispute that this is exactly how the button works, but Plaintiffs press the theory that the (s)WAA button should stop *all* data flow to Google from any Google product or service if Google knows the end user has (s)WAA off — every bit and byte. But that is not what the (s)WAA button representations say. For Plaintiffs to prevail on any of their claims, a reasonable juror would have to conclude that the phrase "to your Google Account" in the (s)WAA description was surplusage, otherwise that limitation must mean *something*, and so it cannot be that the button should stop *all* data flow. Because no reasonable juror can so conclude, Plaintiffs cannot prevail. As a matter of law, they consented.

Finally, Plaintiffs' Motion for Class Certification grossly misused internal e-mails and user studies to suggest that the record-keeping that is now the focus of their case was considered internally at Google and concluded by certain employees to violate the promise of WAA. None of those documents supported Plaintiffs' position, because there is *no* evidence that any Google employee ever believed that the WAA button would somehow disable all advertising by stopping the flow of all data between a mobile app seeking to serve an ad and Google, or disable the logging of basic ad events like conversions. Indeed, each employee and former employee asked about this in deposition denied that they ever shared Plaintiffs' extreme reading of WAA, even as they internally expressed unrelated concerns about WAA that are not a basis for this case.

B. Plaintiffs cannot maintain their privacy torts for independent reasons.

From the start, this case was manufactured around a creative, lawyerly, *unreasonable* reading of the (s)WAA description coupled with the incorrect allegation that Google was collecting personally identifiable (s)WAA-off activity data. It wasn't, it doesn't, and the pseudonymous data it *does* collect is collected lawfully. As a result, the fundamental premise of Plaintiffs' privacy claims, that Google intentionally violated a reasonable expectation of privacy in a highly offensive manner causing harm, has no factual basis. *See Shulman v. Grp. W Prods., Inc.*, 18 Cal. 4th 200, 232 (1998) (reciting elements).

No expectation of privacy. There is no dispute: (s)WAA-off data is not saved to a user's Google Account, and is not associated with any individual user's identity. Instead (s)WAA-off data is logged with random number identifiers that cannot be joined with any person. Courts in this district do not recognize a privacy interest in non-personal information. For example, there is no "protected privacy interest" in a randomly generated "numeric code" that cannot be associated with a user's identity. *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012). And courts have already held that if "app activity data [is] not tied to any personally identifiable information, [is] anonymized, and [is] aggregated," that does not rise to the level of invasion of privacy or intrusion upon seclusion "in this district." *McCoy v. Alphabet, Inc.*, No. 20-CV-05427-SVK, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021). Most recently, a Ninth Circuit panel concluded that Google's clear disclosure in its Privacy Policy that it may receive user activity data across "third-party sites and apps that use Google services," including from the "Android operating system," means users cannot have a reasonable expectation of privacy in their app activity data on Android devices vis-à-vis Google, as these apps utilize the Android OS. *Hammerling v. Google, LLC*, No. 22-17024, (9th Cir. Mar. 5, 2024) (unpublished).

This outcome makes sense. Nobody who uses mobile apps reasonably believes that they can grind the mobile ads ecosystem to a halt by flipping a single button (or any other way). Even when personalization of advertising is disabled, advertising can still be served in spaces where apps choose to sell advertising space. And the server of those apps will of course keep a log that the ad was served. Under Plaintiffs' theory, ads served in a mobile app that were selected *at random*

violated their privacy because they expected the (s)WAA button to disable the entire data flow from the app to Google, no matter how anonymous. That theory cannot square with any reasonable definition of expectation of privacy.

Nor does the (s)WAA toggle set an expectation of privacy in pseudonymous data. The disclosures Google made in its (s)WAA description and its Privacy Policy unambiguously and uniformly explain that (s)WAA controls whether activity data is saved to a user's Google Account, *i.e.*, associated with their identity. Wherever these concepts are discussed in the Privacy Policy, Google's distinction between "your Google Account" and "non-personal information" is clear and unambiguous, and the Privacy Policy also makes clear that privacy controls, including (s)WAA, can toggle whether Google collects personal information, but that it will continue to keep basic records with non-personal information and report that basic record information to advertisers. *See* Privacy Policies, ECF 323-1, at 4–9, 11, 15–17, 23, 52, 54–55, 57 (Appx. A-7). Nor can there be a triable issue here based solely on Plaintiffs' confusion despite these unambiguous disclosures, as that would fatally undermine their class certification theory, which presumes that the class was uniformly exposed to these disclosures and asks the factfinder to determine class-wide whether the class was reasonably confused.

Not highly offensive. Data sent to Google by apps using GA4F is handled consistently with Google's description of (s)WAA. There is no dispute that Plaintiffs were subject to Google's disclosures, and accepted Google's terms of service. Google disclosed the collection of pseudonymous data notwithstanding (s)WAA. No reasonable person would find disclosed and agreed-upon conduct highly offensive.

Per Google's disclosures, a user's app activity data collected via GA4F is never saved to their Google Account (or associated with their personal identity in any other way for that matter) if (s)WAA is off. Nor could the collection of such data be considered "an egregious breach of social norms" or "intrusion [] in a manner highly offensive to a reasonable person." *See also Williams v DDR Media, LLC*, No. 22-cv-03789-SI, 2023 WL 5352896 at *5-6 (N.D. Cal. Aug. 18, 2023); *City & Cnty. of San Francisco v. Purdue Pharma L.P.*, No. 18-CV-07591-CRB, 2021 WL 842574, at *2 (N.D. Cal. Mar. 5, 2021) (holding no privacy concerns in de-identified information in discovery

dispute); *London v. New Albertson's, Inc.*, No. 08-CV-1173 H(CAB), 2008 WL 4492642, at *8 (S.D. Cal. Sept. 30, 2008) (same). Thus, "there is no plausible allegation that [Google] tracked *Plaintiff's* location as opposed to some anonymous clientid that is not matched to any particular person."[22] *Moreno v. San Francisco Bay Area Rapid Transit Dist.*, No. 17-CV-02911-JSC, 2017 WL 6387764, at *4 (N.D. Cal. Dec. 14, 2017) (emphasis in original).

This makes good sense. Google has taken significant steps to bar the very practice that Plaintiffs allege occurred here—the *personal* tracking of a user despite their decision to turn (s)WAA off. Even if it was reasonable for users to review the WAA disclosure and related disclosures and conclude that turning off (s)WAA would prevent Google from retaining any record that it served an ad to a device identifier that is never associated with the user's identity, no reasonable juror could conclude on these facts that Google's retaining such a record is highly offensive, because the record does not identify anything about anyone—a far cry from anything approaching actionable invasion of privacy.

No intent. To the extent a reasonable juror could conclude that there is any daylight between the description of (s)WAA and the Privacy Policy on one hand and Google's uniform conduct on the other hand, no reasonable juror could conclude that Google **intentionally** invaded the privacy of or intruded upon the seclusion of class members. To the contrary, Google took substantial steps—far beyond the steps it was obligated to take—to prevent bad actors and its own employees from invading class members' privacy. Google contractually forbade app developers from sending it personally identifiable information, it instituted technologically sophisticated safeguards to maintain users' identity separate from the app activity data it stored for app developers, and it disabled itself from using the data for any purpose other than those disclosed to users in the Privacy Policy—basic record-keeping about its advertising business (and *not* any ads personalization or building of marketing profiles). Even if a reasonable juror could find that Google's description of the (s)WAA button deviated in some way from Google's uniform conduct, no reasonable juror could conclude that this variance was done with the intent required to commit the intentional tort of

[22] Nor is it sufficient to "postulate that [] third parties could, through inferences, de-anonymize this data" if it is "not clear that anyone has actually done so." *Low*, 900 F. Supp. 2d at 1025.

invasion of privacy. *See Caraccioli v. Facebook, Inc.*, 167 F. Supp. 3d 1056 (N.D. Cal. 2016) (finding that intrusion upon seclusion or intentional infliction of emotional distress claims require intent on the part of the tortfeasor); *see also In re Accellion, Inc. Data Breach Litig.*, No. 5:21-CV-01155-EJD, 2024 WL 333893, at *16 (N.D. Cal. Jan. 29, 2024) (dismissing plaintiffs' intrusion upon seclusion claim where complaint failed to allege that defendant "intentionally intruded" or that the intrusion was highly offensive). As a matter of law, the undisputed facts cannot make out the intent element of the privacy torts.

Because Plaintiffs cannot establish any of the elements of their privacy claims, summary judgment should be granted in Google's favor on those claims.

C. Plaintiffs cannot establish harm for any of their claims.

Harm is a necessary element of the intentional torts and Plaintiffs' CDAFA claim, and Plaintiffs cannot show any harm to the class as a result of Google's conduct. *See Perkins v. LinkedIn Corp.,* 53 F. Supp. 3d 1190, 1219 (N.D. Cal. 2014) (dismissing plaintiffs' CDAFA claims on the basis that Plaintiffs did not adequately allege that they had suffered any "tangible harm from the alleged Section 502 violations"); *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1090 (N.D. Cal. 2022) ("Determining whether a defendant's actions were 'highly offensive to a reasonable person' requires a 'holistic consideration of factors such as the ***likelihood of serious harm*** to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive.'") (quoting *Facebook Tracking*, 956 F.3d at 606 (quoting *Hernandez v. Hillsides, Inc.*, 211 P.3d 1063, 1073 (2009)) (emphasis added).

Google opposed class certification in part on the basis of individualized harm inquiries. The Court rejected that argument and accepted that Plaintiffs could demonstrate class-wide harm, reasoning that "even if Google is right, and the 'vast majority' of class members' data was only exposed to record-keeping 'not tied to a person's identity or used by Google for any purpose other than to perform accounting for the apps that generated the data or advertising in the first place,' Opp., at 16, then surely that can be proven by common evidence of Google's record-keeping practices." ECF No. 352, at 12. Plaintiffs' certified class thus must proceed on a theory that the

money Google made by keeping receipts for the advertising it sold is the appropriate measure of class-wide damages, regardless of whether keeping receipts harmed any individual class member.

The problem with this theory is that Google's conduct cannot be said to have harmed any class member in particular or the class at large, because its conduct did not exploit any class member's privacy, did not intrude upon their private space, or take from them something they intended to keep for themselves or sell to another, *i.e.*, pseudonymous data about their use of Firebase-enabled apps. No court has ever found that such basic record-keeping is harmful to anyone.

To fix this problem, Plaintiffs have previously relied on an entitlement to disgorgement of profits to allege harm under their tort and CDAFA claims, based on a single sentence in the Ninth Circuit's decision in *Facebook Internet Tracking*, 956 F.3d 589. But, as Judge Chhabria has pointed out, the court's analysis on this was solely focused on Article III standing, not the damage or harm required to establish liability under Plaintiffs' tort and CDAFA claims. *See McClung,* 2024 WL 189006, at *2. ("The Court continues to be skeptical of the plaintiffs' theory that California's statutory standing requirement for these claims can be satisfied simply by alleging that the defendant was unjustly enriched by the misappropriation of personal information."). Further, "the Article III analysis in that section of *Facebook Internet Tracking* has been superseded by *TransUnion*, making it even more of a stretch to rely on that section as an implicit statement about statutory standing under California law. *Id.* at n.2 (citing *TransUnion*, 594 U.S. at 426–30).

Finally, to the extent Plaintiffs seek to rely on the subjective experiences of the Named Plaintiffs, that would belie the theory of damages Plaintiffs pushed in order to certify the class. They cannot now backtrack and argue that the idiosyncratic emotional experiences of 100 million class members can be proven class-wide; obviously they cannot be. In other words, Plaintiffs argued themselves into a corner: they cannot tell this Court that they need not prove actual damages in order to certify a class, only to argue now in opposition to summary judgment that they can prove actual class-wide harm using common proof. The two are irreconcilable.

D. Plaintiffs' analysis of the CDAFA claim's "without permission" requirement focuses on the wrong permission-giver.

Plaintiffs' CDAFA claim fails for the reasons discussed above. But the CDAFA claim fails

for the additional reason that Plaintiffs cannot establish that Google acted "without permission," even if app developers' end users failed to consent to their use of GA4F by virtue of their (s)WAA settings, because the most correct lens to view this claim through is one that focuses on Google's permission vis-à-vis the app developers, not the end users.

Google never exceeded the scope of its permission to use the data gathered by app developers and sent to Google via GA4F because it is undisputed that (1) Google required app developers to obtain consent from end users for their use of GA4F (*See* Google's Resps. to Plaintiffs' Interrog., Set Six, ECF No. 364-22, at 10:25–11:18 (Appx. A-22)) and (2) Plaintiffs do *not* allege an invasion of their privacy solely by virtue of Google's function as *data processor* for app developers as their agent. Nor could they: Courts in this district have already held that when a tech company acts as a vendor for another, its scope of consent is coterminous with the party to the communication. *See Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021); *Williams v. What If Holdings, LLC*, No. C. 22-03780 WHA, 2022 WL 17869275, at *3 (N.D. Cal. Dec. 22, 2022); *see also Byars v. Hot Topic, Inc.*, 656 F. Supp. 3d 1051, 1067–68 (C.D. Cal. 2023); *Johnson v. Blue Nile, Inc.*, No. 20-cv-08183-LB, 2021 WL 1312771, at *1 (N.D. Cal. Apr. 8, 2021); *Yale v. Clicktale, Inc.*, No. 20-cv-07575-LB, 2021 WL 1428400, at *3 (N.D. Cal. Apr. 15, 2021).

Here, none of Google's conduct falls outside the scope of its role as vendor for the app developers. Google does not make copies of the (s)WAA-off data for itself to, e.g., enhance its marketing profiles or better personalize advertising. It does not sell or exploit the data. It processes the data sent to it under contracts with third party entities who collected it. And those contracts permit Google to use the data for various uses. Plaintiffs have never alleged that Google exceeded that scope of permission, so no CDAFA claim could lie.

VI. CONCLUSION

For the foregoing reasons, the Court should dismiss this case with prejudice.

Dated: April 4, 2024

Respectfully submitted,

WILLKIE FARR & GALLAGHER LLP

By: */s/ Eduardo E. Santacana*

Benedict Y. Hur
Simona Agnolucci
Eduardo E. Santacana
Argemira Flórez
Harris Mateen

Attorneys for Defendant Google LLC

EXHIBIT 2

WILLKIE FARR & GALLAGHER LLP
BENEDICT Y. HUR (SBN: 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN: 246943)
sagnolucci@willkie.com
EDUARDO E. SANTACANA (SBN: 281668)
esantacana@willkie.com
ARGEMIRA FLÓREZ (SBN: 331153)
aflorez@willkie.com
HARRIS MATEEN (SBN: 335593)
hmateen@willkie.com
333 Bush Street, 34th Floor
San Francisco, CA 94104
Telephone: (415) 858-7400

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ANIBAL RODRIGUEZ, *et al*. individually and on behalf of all others similarly situated,

Plaintiff,

vs.

GOOGLE LLC, *et al*.,

Defendant.

Case No. 3:20-CV-04688 RS

GOOGLE LLC'S MOTION FOR SUMMARY JUDGMENT

Date: July ~~11~~25, 2024
Time: 1:30 p.m.
Courtroom: 3, 17th Floor
Judge: Hon. Richard Seeborg

Action Filed: July 14, 2020
Trial Date: February 10, 2025

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

I. INTRODUCTION

This case started with Plaintiffs' allegation that data generated when users had turned off their Web & App Activity settings "is combined by Google into a user profile with all the other detailed, user-specific data Google collects on individuals and their devices," which "Google then uses [] to help generate billions of dollars in advertising revenues without users' consent." Compl., ECF No. 1[1], at ¶¶ 37–39,141–143, 146. None of that was true. Four years, hundreds of thousands of pages of produced documents, and almost 200 hours of fact and expert deposition testimony later, Plaintiffs have failed to produce a single shred of evidence substantiating that allegation. So, out of the ashes of their original theory, Plaintiffs seek to resurrect their case with the claim that Google should not have kept non-identifiable receipts for the ads it serves. And, the tortured theory goes, had Google not kept those receipts, advertisers would have refused to pay for advertising, so all of Google's advertising profit for ads served to WAA-off users should be forfeited. On that basis, Plaintiffs seek to convert their picayune liability theory into a half-billion dollar demand for class-wide judgment.

Since the allegations of Plaintiffs' current, certified theory—that Google promised not to engage in record-keeping, that Plaintiffs had a reasonable expectation the record-keeping would not occur, and that Plaintiffs suffered harm as a result of the record-keeping—are completely lacking in factual basis, the Court should grant summary judgment and dismiss this case with prejudice.

First, Google repeatedly disclosed and secured the consent for its basic record-keeping practices, which involve logging "non-personal information" for the purpose of reporting how ads and mobile apps are performing.

Second, each Plaintiff saw these disclosures, but argues that the WAA webpage led them to believe they could disable Google's record-keeping by switching WAA to "off." But the WAA webpage describes the button as a way to give or withhold permission for Google to "save" app activity data "to your Google Account" for the purpose of "personaliz[ing]" the user's experience. There is no reasonable interpretation of this language, in isolation or in concert with the Privacy

[1] Google will submit a hard-copy courtesy booklet of selected docket entries that are not listed in Appendix A (Evidentiary Material) or Appendix B (Previously Filed Under Seal Material) for the Court's ease of reference.

Policy, that extends the ambit of the WAA control to Google's non-personal record-keeping. And to the extent it was not immediately obvious from the WAA webpage that "to your Google Account" limited the ambit of the control, the Privacy Policy, which each Plaintiff alleges they reviewed, repeatedly explained that Google distinguishes between personally identifiable information and non-personal information.[2] The information Google used to keep its records was non-personal information, and Google used it in the precise ways it told Plaintiffs it would.

Third, Google did *not* use the information at issue to target or personalize ads, or build marketing profiles of WAA-off users. Plaintiffs originally alleged Google did so, but they never had a basis to make this allegation, and they abandoned that theory at class certification.

Finally, Google's basic record-keeping doesn't hurt anyone. Logging the fact that Google has served an ad to a randomly generated identifier that is never linked to a Google user's identity cannot be said to have exploited any class member's privacy, nor intruded upon their private space, nor taken from them anything they intended to keep for themselves or sell to another.

Nor can Plaintiffs fall back on disgorgement of profits as a basis to establish Article III or statutory standing, nor harm for their privacy torts. While the Ninth Circuit had, in a single sentence, ruled that such claimants can establish Article III standing in *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020), that is no longer good law in the wake of *TransUnion. See TransUnion LLC v. Ramirez*, 594 U.S. 413, 424–25 (2021). Nor did the Ninth Circuit purport to rule on the question of statutory standing or the element of harm required for privacy torts.[3]

---

[2] *See* Declaration of Anibal Rodriguez in Support of Class Certification, ECF No. 315-7, at ¶ 3 (Appx. A-5) ("When I opened my Google account in 2014, and in the years before filing this lawsuit, I had read Google's Terms of Service, Privacy Policy, and other Google disclosures to understand what data was and was not collected when WAA and sWAA were turned off. I agreed to those terms."); Decl. of Sal Cataldo, ECF No. 315-5, at ¶ 3 (Appx. A-3) (same); Decl. of Julian Santiago, ECF No. 315-8 (Appx. A-6) (same); Decl. of Susan Harvey, ECF No. 315-6, at ¶ 3 (Appx. A-4) (same).

[3] *See McClung v. AddShopper, Inc.*, No. 23-cv-01996-VC, 2024 WL 189006, at *2 (N.D. Cal. Jan. 17, 2024) ("The Court continues to be skeptical of the ~~plaintiffs'~~plaintiffs' theory that ~~California's~~California's statutory standing requirement for these claims can be satisfied simply by alleging that the defendant was unjustly enriched by the misappropriation of personal information . . ." and "[T]he Article III analysis in that section of *Facebook Internet Tracking* has been superseded by *TransUnion*, making it even more of a stretch to rely on that section as an implicit statement about statutory standing under California law.") (citing *TransUnion*, 594 U.S. at 426–30); *see also id.* (citing *Hazel v. Prudential Financial, Inc.*, No. 22-cv-07465-CRB, 2023 WL 3933073, at *6 (N.D. Cal. June 9, 2023) ("Just because Plaintiffs' data is valuable in the abstract, and because [a company] might have made money from it, does not mean that Plaintiffs have 'lost money or property' as a result.").

II. PROCEDURAL BACKGROUND

A. Plaintiffs' ~~Original~~original Complaint and Google's Motions to Dismiss

Plaintiffs filed their original complaint against Google LLC and Alphabet Inc. in July 2020, asserting claims for violation of the Federal Wiretap Act, section 631 (wiretap) and 632 (eavesdropping) of the California Invasion of Privacy Act ~~(~~("CIPA~~),~~"), invasion of privacy, and violation of the California Comprehensive Computer Data Access and Fraud Act ~~(~~("CDAFA~~),~~"), Cal. Penal Code § 502 *et seq.* ECF No. 1.[4] Google moved to dismiss in October 2020, ECF No. 48, and Plaintiffs amended their complaint rather than oppose, (First Am. Compl. ("FAC"~~))~~")), ECF No. 60. The FAC added several Plaintiffs, many of whom have since voluntarily withdrawn from the case.[5] The FAC also asserted two more causes of action for violation of the California Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq.* and for common law intrusion upon seclusion.

Google moved to dismiss every claim in the FAC. ECF No. 62. This Court ruled on that motion on May 21, 2021, granting the motion with leave to amend as to Plaintiffs' claims for violation of the Federal Wiretap Act, section 632 of CIPA, and the Unfair Competition Law. ECF No. 109, at 17~~–~~18. Applying Rule 9(b), the Court also dismissed Plaintiffs' theory of the case as to purported "secret scripts" embedded in Google's Android mobile operating system that supposedly facilitated unlawful interceptions of communications, again with leave to amend. *Id.* at 11~~–~~12.

Plaintiffs' Second Amended Complaint ("SAC") dropped the Federal Wiretap Act and Unfair Competition Law claims, and disavowed the "secret scripts" theory, but added a breach of contract claim. ECF No. 113, at 68~~–~~71. Google moved to dismiss again, this time only as to Plaintiffs' claims for breach of contract and violation of section 631 of ~~the Invasion of Privacy Act.~~CIPA. ECF No. 115. This Court granted Google's motion as to both claims, holding that Plaintiffs failed to state a claim for relief as to breach of contract, and that Plaintiffs' allegations established that Google's alleged wrongful use of recorded communications between users and app developers took the alleged conduct outside the ambit of CIPA section 631, since that statute

[4] All references to "ECF" are for docket entries in the above-captioned matter. Google also provides cited ECF entries to the Court in its "Courtesy Copy of Selection of Docket Entries."

[5] The withdrawn Plaintiffs are: Eliza Cambay, Emir Goenaga, JulieAnna Muniz, Julian Santiago, Harold Nyanjom, and Kellie Nyanjom.

requires simultaneous wiretapping for liability. ECF No. 127. In their ~~Second Amended Complaint~~SAC, Plaintiffs ~~had~~ also added factual allegations concerning the integration of Google Analytics for Firebase with AdMob and with Firebase Cloud Messaging. This Court ruled those allegations could stand because Plaintiffs put Google on notice of their allegations that Google Analytics for Firebase and those two products are integrated such that the latter products use data collected by the former. *Id.* at 3, 7~~–~~8.

Plaintiffs filed their Third Amended Complaint ("TAC") on September 1, 2021, re-asserting their breach of contract and CIPA section 631 claims. ECF No. 131 (unredacted at ECF No. 130). Google moved to dismiss those claims again, ECF No. 139, and the Court dismissed them with prejudice. ECF No. 209. Google answered the TAC on February 22, 2022. ECF No. 230.

Finally, in late 2022, two days before discovery closed, Plaintiffs sought to amend their complaint again to add ~~in~~ Google Search as an accused product in the case. ECF No. 258. This Court denied that motion for leave to amend while permitting an unopposed amendment to the extant class definitions. ECF No. 281. The operative Fourth Amended Complaint ("4AC") was filed on January 4, 2023. ECF No. 289.

B. Plaintiffs' ~~Theory~~theory of ~~Liability~~liability on the ~~Pleadings~~pleadings

Through successive orders on Google's motions to dismiss, this Court narrowed Plaintiffs' case to a simple and straightforward claim. As described by the Court in its first Order on Google's Motion to Dismiss the FAC, Plaintiffs allege that Google Analytics ("GA") for Firebase, a tool Google provides to app developers for use on mobile devices, "when functioning as advertised in a given app, contravenes [Google's] user-facing privacy representations." ECF No. 109, at 1. If, as Plaintiffs allege, GA for Firebase ("GA4F") does contravene Google's user-facing privacy representations, this Court ruled, Plaintiffs would have claims against Google for violation of the CDAFA and the common law torts of intrusion upon seclusion and invasion of privacy. *Id.* at 14~~–~~16.

In particular, Google makes available to users "a complex user-facing privacy apparatus" for controlling various privacy-related aspects of the user experience. *Id.* at 2~~–~~4. One such tool is an

account setting (among others) called "Web & App Activity," or WAA. The WAA button[6] "purports to give consumers control over a defined subset of Google's data-gathering efforts." *Id.* at 3. Specifically, it tells users that if they turn on the toggle, that will "let Google save" certain information to "an individual's 'Google Account.'" *Id.* at 3. That set of data comprises "'info about [the individual's] searches and other activity on Google sites, apps, and services,' as well as 'info about [the individual's] . . . activity on sites, apps, and devices that use Google services.'" *Id.* The Court found particularly relevant in these disclosures two undefined terms—"Google services" and "Google Account." Depending on how a user interprets those terms, this Court held, a reasonable user could potentially be misled by the description of the WAA button in light of how ~~GA for Firebase~~GA4F works. *Id.* at 8~~–~~10.

~~GA for Firebase~~GA4F is an enterprise-facing product that app developers can use for free. *Id.* at 4. When functioning as advertised, "GA for Firebase will automatically send various interactions between the app and its users . . . to Google, which will then present a clean, optimization-minded analysis of that data to the developer." *Id.* at 4. To use ~~GA for Firebase~~GA4F, app developers must agree to obtain consent for end users for the developer's use of ~~GA for Firebase.~~GA4F. *Id.* at 4~~–~~5 & n. 3 (discussing "GA for Firebase Materials," a "suite of agreements, policies, and resources" provided to developers in Google's publicly-available online "Help Center~~.""~~"). As described by the Court, Plaintiffs allege that ~~GA for Firebase~~GA4F contravenes the WAA description as follows:

> ~~plaintiffs~~Plaintiffs allege Google's capture and analysis of data via GA for Firebase, on behalf of app developers who knowingly utilize that service, violates the WAA Materials' representations to individuals who have disabled the WAA feature. Under this theory of liability, GA for Firebase—when running as marketed—allows Google to collect information about an individual's "activity on . . . apps . . . that use Google services," notwithstanding the WAA Materials' statement that "[t]o let Google save this information . . . Web & App Activity *must* be on."

[6] Following the Court's May 2021 Order Granting in Part Google's Motion to Dismiss, Plaintiffs amended their complaint to include descriptions of the supplemental Web & App Activity ~~("sWAA~~("(s)WAA") button. *See* 4AC, ECF No. 289~~-~~. The (s)WAA button provides users with the option to allow Google to save "Chrome history and activity from sites, apps, and devices that use Google services" to the user's Google Account. *Id.* at 22. WAA must be on for ~~sWAA~~(s)WAA to be on. *Id.* Thus, when a user disables the WAA toggle, the ~~sWAA~~(s)WAA button is also disabled. *Id.* In this case, the parties refer to the two controls collectively as "WAA" or "(s)WAA~~"~~".

Id. at 6 (emphasis in original). Further, this Court ruled that the phrase "Google Account" was sufficiently ambiguous that a user could reasonably believe that turning WAA off would prevent Google from saving ~~GA for Firebase~~GA4F data linked to that user's "e-mail address," or that "monitors" that user's activity across the web, or that personalizes that user's experiences across Google services. *Id.* at 8~~–~~9. As a result, Plaintiffs stated a claim for violation of the CDAFA because Google's data collection was allegedly "without permission," and for invasion of privacy because the question of whether the user consented and whether the collection was highly offensive were inappropriate for resolution on the pleadings. *Id.* at 14~~–~~16. Those are the claims that have survived through later motions to dismiss. As of today, four named Plaintiffs remain: Sal Cataldo, Susan Lynn Harvey, Anibal Rodriguez, and Julian Santiago. *See* 4AC, ECF No. 289.

C. The ~~Discovery Period~~discovery period

In total, the parties engaged in 48 months of fact discovery and 5 months of expert discovery, comprising 211,186 pages of produced documents, 1,113 pages of expert reports, 2,201 pages of expert depositions, and 4,239 pages of witness deposition transcripts. Santacana Decl~~.~~¶. ¶ 3. When necessary, the parties appealed to Judge Tse to resolve discovery disputes. In all, Judge Tse issued 21 Orders resolving 25 discovery disputes. Santacana Decl. ¶ 3. At the close of fact discovery, Plaintiffs requested a two-month extension of the discovery period on the grounds that Google had engaged in alleged discovery misconduct. ECF No. 279. This Court denied that motion in December 2022. ECF No. 282.

D. The Court's Order ~~Granting~~granting Class Certification

Following expert discovery, Plaintiffs moved for class certification, ECF No. 315, and Google opposed, ECF No. 329. The Court issued its Order granting class certification on January 3, 2024, ECF No. 352, certifying two classes of plaintiffs comprising individuals who turned off (s)WAA and used Firebase~~–~~ ~~–~~or Google Mobile Ads~~–~~-enabled apps.

In order to secure class certification, Plaintiffs disclaimed a variety of arguments and pressed to the Court the theory that the mere collection of app activity data, absent any use by Google, and even if it is made pseudonymous or anonymous, nevertheless contravened Google's description of the WAA button, and that the difference could be used to hold Google liable class-wide.

Accepting Plaintiffs' arguments, the Court granted class certification and rejected Google's arguments concerning individualized issues. *Id.* In particular, the Court reasoned that Google's consent defense could be decided class-wide because "Google's representations about the WAA feature, unambiguous and persistent by its own admission, outweigh these individual questions about *where* class members learned about the WAA feature." *Id.* at 15–16 (emphasis in original). Further, the Court held that "the relevant 'conduct' showing a lack of consent is the users' decisions affirmatively to switch off the WAA and sWAA buttons," which this Court held constituted a "common act representing their privacy choices, based on Google's own ubiquitous representations." *Id.* at 9–10. In addition, the Court held that "even if Google is right, and the 'vast majority' of class members' data was only exposed to record-keeping 'not tied to a person's identity or used by Google for any purpose other than to perform accounting for the apps that generated the data or advertising in the first place,' Opp. at 16, then surely that can be proven by common evidence of Google's record-keeping practices." *Id.* at 12.

III. STATEMENT OF FACTS

The following statement of facts is undisputed. To the extent Plaintiffs dispute any fact below, Google respectfully submits that no evidence in the record supports such a position.

A. Plaintiffs concede that Google does not personalize advertising with (s)WAA-off data; the certified theory of liability challenges basic, pseudonymous record-keeping.

~~GA for Firebase~~GA4F is "an app measurement solution" used by mobile app developers for "insight on app usage and user engagement." *See Google Analytics*, Firebase, ECF No. 324-1(Appx. A-8).[7] Using ~~GA for Firebase~~GA4F, app developers can measure various "events," or specific types of user interactions with their apps.[8] *See* Expert Report of Jonathan Hochman ("Hochman Rpt.,") ECF No. 361-58, ¶¶ 89–91 (Appx. A-11~~) ;);~~ Interrog. Set One Resps., ECF No. 364-1, at 4:20–

[7] *See also* Interrog. Set One Resps., ECF No. 364-1, at 5:8–21; "App Attribution in GAA," ECF No. 364-2, at -515 (Appx. A-14) (Unsealed Version at Appx B-4~~) ;);~~ Hochman Rpt., ECF No. 361-58, at ¶ 62 (Appx. A-11).

[8] Default events include, for example, the first opening of an app, or when a user clicks on a certain part of the app. ECF No. 361-58, ¶ 94 & n. 84; Interrog. Set One Resps., ECF No. 364-1, at 4:20–5:21 (Appx. A-13); *see also* ECF No. 324-4 (excerpting "[GA4] Automatically collected events") (Appx. A-9).

5:6 (Appx. A-13). As a service provider, Google accepts bundles of event data from app developers' apps and stores and analyzes them for those developers regardless of a user's (s)WAA setting. ECF No. 364-1, at 10:15–11:5, 28:4–28:23 (Appx. A-13).

As long as they comply with Google's terms of use, app developers can also customize their usage of GA4F. *See* Historic GA4F Terms of Service (Appx. A-2); ECF No. 65, at 5–6 (Appx. A-1).[9] Per Google's terms, apps must disclose and obtain consent from end users to use the SDK. *Id.*

In their complaints, Plaintiffs alleged that Google saves WAA-off data to marketing profiles and uses them to personalize advertising, that Google "includes in its user profiles" data "secretly transmitted to Google" by "tracking and advertising code," *i.e.* GA4F. And they claimed that by "including this data in its user profiles, Google increases the user profiles' value" and "allows Google to more effectively target advertisements to these users"; and that "this [sWAA-off] data is combined by Google into a user profile with all the other detailed, user-specific data Google collects on individuals and their devices," which "Google then uses [] to help generate billions of dollars in advertising revenues without users' consent." ECF No. 1, ¶¶ 37–39, 141–143, 146.

Over the course of this lawsuit, Plaintiffs' narrative shifted; they and their experts now concede these allegations were false.[10] Indeed, Google's verified interrogatory response, served nearly three years ago, made it clear: **Google does not save WAA-off data to any Google user's marketing profile, and does not use WAA-off data for personalized advertising, either in connection with a user's true identity *or* in connection with a user's pseudonymous identity.**[11] Interrog. Set One Resps., ECF No. 364-1, at 7:7–14 (Appx. A-13). Plaintiffs no longer contend, as they once did, that Google secretly collects (s)WAA-off data to create profiles for personalized

[9] *See also* Additional Historic GA4F Terms of Service, (Appx A-2).

[10] *See* Dep. Tr. of Jonathan Hochman ("Hochman Tr."), ECF No. 364-19, at 194:18–24 (Appx. A-20) (Q. "[Y]ou're not disputing in this case that Google will not personalize ads . . . with sWAA-off Google analytics for Firebase data?" A. "That's correct."). *See also* Dep. Transcript of Michael Lasinski ("Lasinski Tr."), ECF No. 364-17, at 79:16–18 (Appx. A-19) ("[M]y understanding is that Google has represented that sWAA-off users do not receive personalized ads."); *id.* at 81:6–9 (Q. "So for neither scenario did you assume that sWAA-off users were receiving personalized ads that relied on sWAA-off data?" A. "Correct.").

[11] *See also* Google's Resps. to Plaintiffs' Interrog., Set Six, ECF No. 364-22, at 8:21–10:9 (Appx. A-22); Interrog. Set One Resps., ECF No. 364-1, at 23:15–25:23 (Appx. A-13); Interrog. No. 18 Resps., ECF No. 364-8, at 5–6; Dep. Tr. of Belinda Langner ("Langner Tr."), ECF No. 364-7, at 78:2–7 (Appx. A-18).

advertising. Instead, Plaintiffs argue that Google uses (s)WAA-off data for basic record-keeping. And, in their Motion for Class Certification, ~~Plaintiffs'~~Plaintiffs paradoxically argued that Google conceals its basic record-keeping with (s)WAA-off data "by turning off 'personalized' ads that could tip [users] off to Google's continued tracking." Class Cert. Mot., ECF No. 361-1, at 2. That is, for most of the pendency of this case, Plaintiffs maintained that Google's alleged personalization of advertising with (s)WAA-off data was deceptive; now they argue that Google's decision not to personalize advertising with (s)WAA-off data is deceptive.

Specifically, the Motion argued that Google contravenes its representations because, even when a user's (s)WAA is turned off, Google will still (1) log the fact that it has served an ad alongside a device identifier for accounting purposes, and (2) attribute conversion events to those ad serving records. *See* ECF No. 361-1, at 14. Plaintiffs' damages theory relied upon to obtain class certification focuses on this use of (s)WAA-off data, positing that (1) "[i]f Google did not collect and save ad requests, it could not serve ads. And without data regarding both ad requests and the ads that Google served, Google would lack the records it needs to charge advertisers for its services" and (2) "Google also uses this ads data to track conversions; if it lacked data regarding a user's interaction with an ad, it would be unable to determine whether that interaction is related to any later behavior." Hochman Rpt., ECF No. 361-58, ¶ 122 (Appx. A-11).[12] The logging of the (s)WAA-off record of ad service or analytics conversion events is, in Plaintiffs' view, an indispensable link in a long chain that ends in advertisers paying for advertising.[13] Thus, Plaintiffs claim, Google should be disgorged of *all* profit made from serving any ads to (s)WAA-off users on mobile apps,

[12] *See ~~also~~ id.* ¶ 271 ("[B]ut for Google's collection of WAA-off or sWAA-off data, Google would not be able to serve advertisements to those users and then charge the advertisers because Google would lack the necessary data records to back up their advertising charges."); Lasinski Tr, ECF No. 364-17, 113:1-3, 113:20-23 (Appx. A-19) ("The advertiser would pay less to Google because Google did not – would not serve an ad in those cases. . . . [T]hey would pay them less because those ads that are currently being shown to sWAA-off users would not be shown to sWAA-off users."); *id.* at 137:8-14 ("My understanding is, based on input given to me, is that Google would not be able to serve an ad in those situations. Whether or not you want to call it an ad blocker, I've never called it that, but Google would not be able to serve an ad in those situations.").

[13] Plaintiffs have also complained that Google uses the (s)WAA-off data to improve Google's products and services (Class Cert. Mot., ECF No. 361-1, at 3), and engage in fraud and spam detection (Hochman Tr., ECF No. 364-19, at 204:25-209:10 (Appx. A-20)), but they do not assign these uses any value in their damages models and do not rely on these arguments to demonstrate class-wide injury.

because to perform the serving of the ad, Google had to exchange information with the mobile app where the ad was served, and keep a record that it served it. *Id.* at ¶ 271; Lasinski Tr., ECF No. 364-17, at 129:12–18 (Appx. A-19).

At a technical level, the practice Plaintiffs complain of as profit-making is the use of (s)WAA-off records by Google to perform "attribution"[14] for advertisers. *See* Hochman Rpt., ECF No. 361-58, ¶¶ 279–296 (describing generally "Attribution/Conversion Tracking"); Appendix E to Hochman Report: Ad Campaigns and Conversion Tracking/Modeling (Appx. A-11); ECF No. 361-59, ¶¶ 12–26 (Appx. A-12) (Unredacted at Appx. B-1). Attribution can be performed in a number of ways. The specific technique Plaintiffs complain of works as follows:

1. **At Time 1**, an ad for the New York Times (NYT) app appears in the Nike app, which uses the Google Mobile Ads SDK (AdMob) to serve ads. An unidentified user clicks on it, causing the SDK to **log that the user's device ID clicked on that ad**.

2. Then, the user installs and opens the advertised NYT app. The NYT app uses the Firebase SDK and GA4F. As a result, **at Time 2**, the NYT app uses GA4F to **log that the user's device ID triggered the "first_open" analytics event**.

3. Google's ad system connects the dots on the back end: the same device ID that clicked on the ad at Time 1 triggered the "first_open" event at Time 2. If the two times are within a time period set by the advertiser (for example, 7 days), Google reports to the app developer/advertiser that **a conversion has occurred**. Over time, the app developer/advertiser receives aggregate reporting on the conversions they've achieved.

Measuring conversions varies from app to app because app developers can choose to rely on Google's default conversion events, like "first_open," or they can create their own custom conversion events.[15] Hochman Rpt., ECF No. 361-58 at ¶ 94 & n.84 (Appx A-11); *see also* "Log Events," Google Analytics (Appx. A-23). Plaintiffs have never offered any explanation for how this basic record-keeping activity harms users.

The conversion and ads logs in question are streamlined to contain just the critical pieces of information—which device triggered the event, the name of the event, which app sent Google the information, and other similar pieces of information. *See* Expert Report of John Black ("Black

[14] *See generally* "Attribution (Marketing)," Wikipedia, The Free Encyclopedia (last modified February 10, 2024), https://en.wikipedia.org/wiki/Attribution_(marketing).

[15] *See generally* "[GA4] Create or Modify Conversion Events," Google Analytics Help, accessed March 21, 2024, https://support.google.com/analytics/answer/12844695?hl=en

Rpt."), ECF No. 364-20, ¶ 92 (Appx. A-21); *see also* Hochman Rpt, App'x E, ECF No. 361-59 (Appx. A-12). So, for example, while a conversion event could be called "in_app_purchase," and it could contain for the app developer pseudonymous information about what the device purchased, for Google's attribution purposes, it is just the fact that the event occurred that is logged and later used to connect an ad click at Time 1 with a purchase at Time 2. *See* Black Rpt., ECF No. 364-20, ¶ 92 (Appx. A-21~~).~~;); *see also* Hochman Rpt., ECF No. 361-58, ¶¶ 122–123.

This accounting function is the basis for the certified theory of liability.

B. Google represented that the WAA button controlled whether data would be "saved to your Google Account," *i.e.*, "associated with your personal information."

The theory of liability certified by this Court centers around Google's representation that turning WAA[16] on would enable Google to "save" a user's activity data "in your Google Account." 4AC, ECF No. 289, at 27. Plaintiffs reason that the opposite should hold true as well; that is, if a user turns off WAA, that should disable Google from saving a user's activity data to that user's Google Account. As discussed below, that is exactly how WAA works.

Part of Plaintiffs' theory of liability rests on the term "**your Google Account**." This is a defined term. *See* Privacy Policies, ECF No. 323-1, at 52 (Appx. A-7). The Privacy Policy ~~(~~("PP~~)~~") has, since the start of the class period, explained that Google treats information "associated with your Google Account" as "personal information," which is distinct from "non-personally identifiable information." Privacy Policies, ECF No. 323-~~1at~~1, at 5, 52 (Appx. A-7). First, the PP explained that "Information we collect when you are signed in to Google, in addition to information we obtain about you from partners, may be associated with your Google Account. **When information is associated with your Google Account, we treat it as personal information.** For more information about how you can access, manage or delete information that is associated with your Google Account, visit the Transparency and choice section of this policy." *Id*. at 5; *see also id*.

[16] The (s)WAA control can only be enabled if WAA is also enabled.

at 6–7, 11 ("Depending on your account settings, your activity on other sites and apps may be **associated with your personal information**" and Google "may share non-personally identifiable information publicly and with our partners.").

Throughout the class period, the PP directed users to a "Key Terms" section if there were phrases they did not understand: "We've tried to keep it as simple as possible, but if you're not familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first." *Id*. at 1. The Key Terms section in turn defined throughout the class period the phrases "Google Account," "personal information," and "non-personally identifiable information." *Id*. at 52. "**Google Account**" was defined as the Account a user signs up for by "providing us with some personal information" which can be used "to authenticate you when you access Google services; "**personal information**" was defined as information "which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google, **such as information we associate with your Google account**;"; and "**non-personally identifiable information**" was defined as "information that is recorded about users so that it no longer reflects or references an individually identifiable user." *Id.* No section of the PP or the WAA page itself suggests to users that there is an account control to disable Google's collection or use of "non-personally identifiable information."[17]

C. Google's disclosures uniformly and unambiguously explained that it could use non-personal information for basic record-keeping.

Google discloses its uses of analytics and ads data in many contexts, and explains the difference between run-of-the-mill record-keeping using non-personal information and personalized advertising using personal information associated with a Google Account.

[17] Further, since at least 2016, in a section linked from the PolicyPP called "How Google uses data when you use our partners' sites or apps," Google explained that "apps that partner with Google can send us information such as the name of the app and an identifier that helps us to determine which ads we've served to other apps on your device. If you are signed in to your Google Account, and depending on your Account settings, we may add that information to your Account, and treat it as personal information." ECF No. 323-1, at 54 (excerpting "How Google uses data when you use our partners' sites or apps" from Google's Privacy & Terms dated June 28, 2016 PP) (Appx. A-7). The account setting referenced here is, once again, the WAA setting.

First, in its Privacy Policy, Google explained throughout the class period that Google uses "cookies or similar technologies to identify your browser or device" and to "collect and store information when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites," including "Google Analytics." ECF No. 323-1, at 4–5. (Appx. A-7). Further, the PP explained that analytics helps app owners "analyze the traffic to their [] apps" and "[w]hen used in conjunction with our advertising services . . . Google Analytics information is linked, by the Google Analytics customer or by Google, using Google technology, with information about visits to multiple sites." *Id.* at 5.

The PP also explained that "we [Google] regularly **report to advertisers on whether we served their ad** to a page and **whether that ad was likely to be seen**." *Id.* at 23. Google's Privacy Portal also hosts a "How Ads Work" page, which again explained: "We give advertisers data about their ads' performance, but we do so without revealing any of your personal information." *Id.* at 29. Starting in March 2018, Google maintained a PP "Technologies" page, a corollary to the earlier "How Ads Work" page; that page again explained: "We store a record of the ads we serve in our logs"; "We anonymize this log data by removing part of the IP address (after 9 months) and cookie information (after 18 months)"; and "You can use Ads Settings to manage the Google ads you see and opt out of Ads Personalization," but "**[e]ven if you opt out of Ads Personalization, you may still see ads** based on factors such as your general location derived from your IP address, your browser type, and your search terms." *Id.* at 49.

Indeed, Plaintiff Sal Cataldo understood that (s)WAA was not an ad blocker and that while he could control ads personalization, he could not use (s)WAA or the ads personalization button to prevent Google from serving ads at all. Dep. Transcript of Sal Cataldo ("Cataldo Tr."), ECF No. 364–6, at 152:18–153:18 (Appx. A-17).

Plaintiffs have argued that the (s)WAA control should function as an ad blocker, and prevent Google even from keeping basic record-keeping of the ads it serves on behalf of third party advertisers. But there is no textual basis for this argument.

Throughout the class period, the PP explained that users can "[r]eview and update your Google activity controls to decide what types of data, such as videos you've watched on YouTube

or past searches, you would like **saved with your account** when you use Google services." ECF No. 323-1, at 7 (Appx. A-7). The text of the WAA control explains: "The data ***saved in your account*** helps give you more ***personalized*** experiences across all Google services. Choose which settings will save data ***in your Google Account***." 4AC, ECF No. 289, at 27 (emphasis added).

Google repeatedly explained to users that they could affect the advertising Google serves to them via the "Ad Settings" button, ***not*** the WAA toggle. The PP and related disclosures made clear that turning off the personalization setting would not prevent Google from serving ads, only make the ads less relevant. ECF No. 323-1, at 48–50 (Appx. A-7). In other words, Google disclosed that it would still perform its role as record-keeper for advertisers, and it would still serve ads, regardless of a user's Google Account Ad or WAA settings (and never represented that activity controls like WAA would have anything to do to the contrary).

D. Google never "saves to a user's Google Account," *i.e.*, personally identifies, (s)WAA-off Analytics or Ads data.

The WAA button says it can be used to give Google permission to save activity data to a user's Google Account. The button does exactly what it says it will do. When WAA is off, Google ***never*** saves activity data to a user's Google account. *See* Interrog. Set ~~1~~One Resps., ECF No. 364-1, at 11:19–13:17 (Appx. A-13); Interrog. Set ~~7~~Seven Resps, ECF No. 364-8, at 6:16–7:26; Hochman Rpt., ECF No. 361-58, at ¶ 205 & n.136 (Appx. A-11); Langner Tr., ECF No. 364-7, at 78:2–78:7 (Appx. A-18).

If the user's (s)WAA toggle—the toggle that applies to data from third-party apps—is set to "off," these data are ***never*** used by Google to identify users; they are processed and analyzed for the benefit of the app developer who generated the data, so they can better understand their own interactions with their own users and the success of their own advertising. Interrog. No. 1 Resps., ECF No. 364-1, at 16:19–17:5, 28:4–29:7 (Appx. A-13). Further, (s)WAA-off data is treated by Google strictly as pseudonymous data. *Id.*; *see* ~~*also*~~ Dep. Transcript of Steve Ganem ("Ganem Tr.") ECF No. 364-3, at 44:16–19 (Appx. A-15). Google logs analytics and ads data alongside a randomly generated pseudonymous identifier (a device ID like ADID or IDFA on iOS) that is never mapped to the identity of the Google Account that was using the device. Interrog. No,

1 Resps., ECF No. 364-1, at 12:7–13:2 (Appx. A-13). Google never unmasks pseudonymous identifiers, and takes steps to ensure these pseudonyms are never re-unified to a user's identity. *Id.* at 8:2–9, 13:3–14:2, 23:15–25:23, 26:11–28:2; App'x X4 to Black Rpt., (sampling Google's "Anti-Fingerprinting" and User Data Access Policies) (Appx. A-16). The only circumstance in which Google saves *any* activity data to a user's Google account is when Google has first ensured the user has provided all required consents, including that (s)WAA is set to "on." Interrog. No. 1 Resps., ECF No. 364-1, at 23:15–26:9 (Appx. A-13)

Plaintiffs do not contest any of this; indeed, when asked about this practice, Plaintiffs' technical expert conceded that Google "has the best intentions here" to keep pseudonymous and identifiable data separate, but complains that "maybe Google is nice today but they become evil in the future" and decides to re-unify data for a government or for profit.[18] Hochman Tr., ECF No. 364-19, at 364:18–365:5 (Appx. A-20).

E. Google has erected technical barriers to the joining of (s)WAA-off data with GAIA-keyed data.

Google takes significant steps to ensure that (s)WAA-off data are not re-associated with the user whose device generated the data. These steps vary from simple isolation of access to critical pieces of information to advanced cryptographic techniques that makes it a practical impossibility for anyone at Google or anyone else to be able to rejoin pseudonymous data to a user's identity.

First, when Google's servers perform a consent check to determine a user's (s)WAA setting, the device IDs are encrypted, and the server checking the user's consent status does not also receive the analytics data. *See* Interrog. No. 1 Resps., ECF No. 364-1, at 23:15–25:6, 26:11–28:2 (Appx. A-13). As a result, the physical machine that receives the encrypted device ID from user devices isn't able to decrypt it, and the physical machine that decrypts the device ID doesn't receive the measurement data. *Id.*

When a consent check returns a (s)WAA-off result, analytics data are logged to

[18] Even if there is a potential for rare instances of violation of Google's terms of service by app developers, that is *not* the basis of any certified theory of liability in this case, as any such idiosyncrasy could not be said to be uniform across the class, nor could Google be held liable for it, since causation would in that case depend on a third party's conduct.

"pseudonymous space." *Id.*, at 23:27–24:7, 25:7–8. These logs do not contain identifying information in them. For example, they do not contain GAIA IDs, which correspond to a user's Google Account identifier. *Id.* at 25:25–26:9. Likewise, GAIA-keyed logs in "GAIA space" at Google do not contain the identifiers in pseudonymous logs, such as device ID or unencrypted app_instance_id. *Id.* Further, for those pieces of information that overlap between the GAIA log and the pseudonymous log, they are encrypted differently and the decryption keys are thrown away after six days, making it impossible to match up fields in one log to the other. *Id.* at 27:8–21.

Google limits access to these decryption keys to select individuals, and if any unauthorized individual seeks access to them, Google has systems in place that will prevent them from obtaining access. *See* Interrog. Set One Resps., ECF No. 364-1, at 27:15–28:2 (Appx. A-13); *see also* Black Rpt., ECF No. 364-20, at ¶¶ 171, 178 (Appx. A-21). Google also "salts" data in GAIA logs, meaning random data is added to it, to make it even harder to match it up to overlapping data sets in pseudonymous logs. ECF No. 364-1, at 26:7–9 (Appx. A-13).

Finally and most importantly, Google employees are flatly forbidden from performing a "join" of data that would unmask the identity of an individual whose data was logged in pseudonymous space. *Id.*, at 24:9–15, 27:22–28:2.[19] Many of these controls have been in place since Google launched ~~GA for Firebase~~GA4F; others have been adopted over time. Google's prohibition on circumventing these privacy controls, however, have been in place at least since ~~GA for Firebase~~GA4F launched. *See* App'x X4 to Black Rpt. (compiling "Anti-Fingerprinting" Policies as far back as January 21, 2015) (Appx. A-16).

IV. UNDISPUTED MATERIAL FACTS

In light of the foregoing statement of facts, and for the ease and convenience of the Court, Google submits that the following undisputed material facts resolve this dispute in its entirety, understanding the Court may also find other undisputed facts described above material as well.

[19] *See also* App'x X4 to Black Rpt., ECF No. 364-4 (Appx A-16) (compiling Google's "Anti-Fingerprinting" Policies); "GEO Privacy Champion"", ECF No. 361-13, at - 411 (Appx. A-10); ECF No. 314-7, (Unsealed Version, Appx B at B-2~~) ;);~~ Ganem Tr., at 44:1-44:19, (Appx. A-15); Hochman Tr., ECF No. 364-19, at 135:25–136:1 (Appx. A-20) ("Yeah, I don't think I necessarily found an indication of joining.").

1. At all relevant times, Google represented that the WAA button controlled whether certain data would be "saved to your Google Account."

2. At all relevant times, the phrase "saved to your Google Account" limited the ambit of the WAA button to permissions relating to saving data in a manner that was associated with personal information.

3. At all relevant times, Google represented through its Privacy Policy and Privacy Portal that the phrase "saved to your Google Account" meant "associated with your personal information," not "saved" in any form, for any purpose, even if made pseudonymous.

4. At all relevant times, Google's Privacy Policy defined "personal information" to mean information "which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google, such as information we associate with your Google account," or a substantially similar definition.

5. Google did not save the WAA-off or (s)WAA-off data at issue in this case generated by class members to that class member's Google Account.

6. Google did not associate the WAA-off or (s)WAA-off data at issue in this case generated by class members with the class members' personal information.

7. Google maintained the WAA-off or (s)WAA-off data at issue in this case generated by class members in pseudonymous or anonymous form in a manner that disabled Google employees from personally identifying the user that generated the data.

8. Google never used the WAA-off or (s)WAA-off data at issue in this case generated by class members to personalize advertising to class members or build marketing profiles.

V. ARGUMENT

Plaintiffs' case hinges on the factual claim that Google saved app activity data gathered by ~~GA for Firebase~~GA4F to Plaintiffs' Google Accounts while (s)WAA was switched off. Because Google represented that it would save such data to a user's Google Account only when they had turned WAA on, Plaintiffs argue, Google violated its promises to users and thereby their privacy rights. That same theory underlies the Court's decision to permit some of Plaintiffs' claims to proceed past the pleadings stage. ECF No. 109, at 3~~–~~4, 6. Per the Court, "[u]nder this theory of liability, ~~GA for Firebase~~GA4F—when running as marketed—allows Google to collect information about an individual's 'activity on . . . apps . . . that use Google services,' notwithstanding the WAA Materials' statement that '[t]o let Google save this information . . . Web & App Activity must be on~~.~~".'" *Id.* at 6. (original emphasis and alterations).

And the same theory is what ultimately was certified by the Court for a class trial. ECF No. 352. In particular, the Court accepted Plaintiffs' argument that the only questions necessary to decide this case are (1) what Google represented, (2) what Google's uniform conduct was, and (3) whether any variance between them rises to the level of liability. *E.g., id.* at 11.

The answers to these three questions are straightforward. (1) Google represented that the WAA button would control whether Google had permission to save activity data to the user's Google Account. (2) Google does not save activity data to the user's Google Account when (s)WAA is off. And (3) Google's practice of keeping basic, pseudonymous records of its advertising does not deviate from its representations concerning (s)WAA. Therefore, there is no liability under the CDAFA or Plaintiffs' invasion of privacy claims.

A. Plaintiffs consented.

Consent is an absolute defense to each of Plaintiffs' remaining claims: CDAFA, invasion of privacy, and constitutional invasion of privacy. Because no reasonable juror could find that Plaintiffs reasonably believed (s)WAA did what they claim, Google's consent defense alone requires a full dismissal of Plaintiffs' claims.

In granting class certification, this Court accepted Plaintiffs' argument that "express consent does not defeat predominance because the "'sWAA disclosures and Google's Privacy Policy' are the only relevant materials for analysis, and are 'the same for all class members.'" ECF No. 352, at 15 (quoting Plaintiffs' Class Cert. Reply, at 10). The Court held that Google's consent defense could be decided class-wide because "Google's representations about the WAA feature, unambiguous and persistent by its own admission, outweigh these individual questions about where class members learned about the WAA feature."[20] *Id.* at 15–16.

Now is the time to make that determination. Plaintiffs by their own argument invited an evaluation of these two sets of uniform representations. If these representations are unambiguous,

[20] Google also argued that class members consented in various ways to Google's conduct by consenting to third party apps' privacy policies. This Court ruled that such consent was not relevant to Google's liability, which could be determined class-wide, because "the relevant question concerns Google's disclosures about the sWAA button, not third-party disclosures to users," and "[t]o the extent Google had a policy that required third party apps to disclose Google's policies to users, that evidence may be applied across the class." ECF No. 352, at 17. As such, these third party disclosures cannot now create a material issue of disputed fact.

or are not susceptible to Plaintiffs' reading of them, their case must end.

The representations are unambiguous. As discussed above, the description of (s)WAA was plain and straightforward: the button controls whether Google has permission to "save" "web & app activity data" to a user's "Google Account."[21] Google does not "save" "app activity data" sent to it via ~~GA for Firebase~~GA4F or the Google Ads products in question, or any product or service addressed by Plaintiffs, to a user's "Google Account." *See* Interrog. Set One Resps., ECF No. 364-1, at 23:27–24:7 (Appx. A-13). Instead, Google's uniform policy and practice is to take significant steps to separate (s)WAA off data from any personally identifiable information belonging to the end user who generated the data. *See id*. at 24:5–28:2, & App'x X4 to Black Rpt., (Appx. A-16).

To the extent any user was confused by the plain meaning of the (s)WAA representations, they were also uniformly presented with Google's Privacy Policy and Privacy Portal, which repeated the distinction between data saved to a "Google Account" and data that is not "associated with personal information" in numerous places. *See supra* III.B. (discussing historic representations made in Google's Privacy Policies, ECF No. 323-1 (Appx. A-7)).

There is no ambiguity to be exploited here. For four years, Plaintiffs have repeated their constant refrain that "off" means "off"; that (s)WAA was a light switch, and that whatever (s)WAA meant, turning it off should do the opposite of what turning it on does. There is no dispute that this is exactly how the button works, but Plaintiffs press the theory that the (s)WAA button should stop *all* data flow to Google from any Google product or service if Google knows the end user has (s)WAA off — every bit and byte. But that is not what the (s)WAA button representations say. For Plaintiffs to prevail on any of their claims, a reasonable juror would have to conclude that the phrase "to your Google Account" in the (s)WAA description was surplusage, otherwise that limitation must mean *something*, and so it cannot be that the button should stop *all* data flow. Because no reasonable juror can so conclude, Plaintiffs cannot prevail. As a matter of law, they consented.

Finally, Plaintiffs' Motion for Class Certification grossly misused internal e-mails and user studies to suggest that the record-keeping that is now the focus of their case was considered

[21] There is also a use limitation in how (s)WAA is described: that the permission is for using the data to "personalize experiences" across Google. Compl., ECF No. 1, at ¶ 49.

internally at Google and concluded by certain employees to violate the promise of WAA. None of those documents supported Plaintiffs' position, because there is *no* evidence that any Google employee ever believed that the WAA button would somehow disable all advertising by stopping the flow of all data between a mobile app seeking to serve an ad and Google, or disable the logging of basic ad events like conversions. Indeed, each employee and former employee asked about this in deposition denied that they ever shared Plaintiffs' extreme reading of WAA, even as they internally expressed unrelated concerns about WAA that are not a basis for this case.

B. Plaintiffs cannot maintain their privacy torts for independent reasons.

From the start, this case was manufactured around a creative, lawyerly, *unreasonable* reading of the (s)WAA description coupled with the incorrect allegation that Google was collecting personally identifiable (s)WAA-off activity data. It wasn't, it doesn't, and the pseudonymous data it *does* collect is collected lawfully. As a result, the fundamental premise of Plaintiffs' privacy claims, that Google intentionally violated a reasonable expectation of privacy in a highly offensive manner causing harm, has no factual basis. *See Shulman v. Grp. W Prods., Inc.*, 18 Cal. 4th 200, 232 (1998) (reciting elements).

No expectation of privacy. There is no dispute: (s)WAA-off data is not saved to a user's Google Account, and is not associated with any individual user's identity. Instead (s)WAA-off data is logged with random number identifiers that cannot be joined with any person. Courts in this district do not recognize a privacy interest in non-personal information. For example, there is no "protected privacy interest" in a randomly generated "numeric code" that cannot be associated with a user's identity. *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012). And courts have already held that if "app activity data [is] not tied to any personally identifiable information, [is] anonymized, and [is] aggregated," that does not rise to the level of invasion of privacy or intrusion upon seclusion "in this district." *McCoy v. Alphabet, Inc.*, No. 20-CV-05427-SVK, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021). Most recently, a Ninth Circuit panel concluded that Google's clear disclosure in its Privacy Policy that it may receive user activity data across "third-party sites and apps that use Google services," including from the "Android operating system," means users cannot have a reasonable expectation of privacy in their app activity data on Android

devices vis-~~aà~~-vis Google, as these apps utilize the Android OS. *Hammerling v. Google, LLC*, No. 22-17024, (9th Cir. Mar. 5, 2024) (~~Unpublished~~unpublished).

This outcome makes sense. Nobody who uses mobile apps reasonably believes that they can grind the mobile ads ecosystem to a halt by flipping a single button (or any other way). Even when personalization of advertising is disabled, advertising can still be served in spaces where apps choose to sell advertising space. And the server of those apps will of course keep a log that the ad was served. Under Plaintiffs' theory, ads served in a mobile app that were selected *at random* violated their privacy because they expected the (s)WAA button to disable the entire data flow from the app to Google, no matter how anonymous. That theory cannot square with any reasonable definition of expectation of privacy.

Nor does the (s)WAA toggle set an expectation of privacy in pseudonymous data. The disclosures Google made in its (s)WAA description and its Privacy Policy unambiguously and uniformly explain that (s)WAA controls whether activity data is saved to a user's Google Account, *i.e.*, associated with their identity. Wherever these concepts are discussed in the Privacy Policy, Google's distinction between "your Google Account" and "non-personal information" is clear and unambiguous, and the Privacy Policy also makes clear that privacy controls, including (s)WAA, can toggle whether Google collects personal information, but that it will continue to keep basic records with non-personal information and report that basic record information to advertisers. *See* Privacy Policies, ECF 323-1, at 4~~–~~–9, 11, 15~~–~~–17, 23, 52, 54~~–~~–55, 57 (Appx. A-7~~)).~~). Nor can there be a triable issue here based solely on Plaintiffs' confusion despite these unambiguous disclosures, as that would fatally undermine their class certification theory, which presumes that the class was uniformly exposed to these disclosures and asks the factfinder to determine class-wide whether the class was reasonably confused.

Not highly offensive. Data sent to Google by apps using ~~GA for Firebase~~GA4F is handled consistently with Google's description of (s)WAA. There is no dispute that Plaintiffs were subject to Google's disclosures, and accepted Google's terms of service. Google disclosed the collection of pseudonymous data notwithstanding (s)WAA. No reasonable person would find disclosed and agreed-upon conduct highly offensive.

Per Google's disclosures, a user's app activity data collected via ~~GA for Firebase~~GA4F is never saved to their Google Account (or associated with their personal identity in any other way for that matter) if (s)WAA is off. Nor could the collection of such data be considered "an egregious breach of social norms" or "intrusion [] in a manner highly offensive to a reasonable person." *See also Williams v DDR Media, LLC*, No. 22-cv-03789-SI, 2023 WL 5352896 at *5-6 (N.D. Cal. Aug. 18, 2023~~),~~); *City & Cnty. of San Francisco v. Purdue Pharma L.P.*, No. 18-CV-07591-CRB, 2021 WL 842574, at *2 (N.D. Cal. Mar. 5, 2021) (holding no privacy concerns in de-identified information in discovery dispute); *London v. New Albertson's, Inc.*, No. 08-CV-1173 H(CAB), 2008 WL 4492642, at *8 (S.D. Cal. Sept. 30, 2008) (same). Thus, "there is no plausible allegation that [Google] tracked *Plaintiff's* location as opposed to some anonymous clientid that is not matched to any particular person."[22] *Moreno v. San Francisco Bay Area Rapid Transit Dist.*, No. 17-CV-02911-JSC, 2017 WL 6387764, at *4 (N.D. Cal. Dec. 14, 2017) (emphasis in original).

This makes good sense. Google has taken significant steps to bar the very practice that Plaintiffs allege occurred here—the *personal* tracking of a user despite their decision to turn (s)WAA off. Even if it was reasonable for users to review the WAA disclosure and related disclosures and conclude that turning off (s)WAA would prevent Google from retaining any record that it served an ad to a device identifier that is never associated with the user's identity, no reasonable juror could conclude on these facts that Google's retaining such a record is highly offensive, because the record does not identify anything about anyone—a far cry from anything approaching actionable invasion of privacy.

No intent. To the extent a reasonable juror could conclude that there is any daylight between the description of (s)WAA and the Privacy Policy on one hand and Google's uniform conduct on the other hand, no reasonable juror could conclude that Google **intentionally** invaded the privacy of or intruded upon the seclusion of class members. To the contrary, Google took substantial steps—far beyond the steps it was obligated to take—to prevent bad actors and its own employees from invading class members' privacy. Google contractually forbade app developers from sending it

[22] Nor is it sufficient to "postulate that [] third parties could, through inferences, de-anonymize this data" if it is "not clear that anyone has actually done so." *Low*, 900 F. Supp. 2d at 1025.

personally identifiable information, it instituted technologically sophisticated safeguards to maintain users' identity separate from the app activity data it stored for app developers, and it disabled itself from using the data for any purpose other than those disclosed to users in the Privacy Policy—basic record-keeping about its advertising business (and *not* any ads personalization or building of marketing profiles). Even if a reasonable juror could find that Google's description of the (s)WAA button deviated in some way from Google's uniform conduct, no reasonable juror could conclude that this variance was done with the intent required to commit the intentional tort of invasion of privacy. *See Caraccioli v. Facebook, Inc.*, 167 F. Supp. 3d 1056 (N.D. Cal. 2016) (finding that intrusion upon seclusion or intentional infliction of emotional distress claims require intent on the part of the tortfeasor); *see also In re Accellion, Inc. Data Breach Litig.*, No. 5:21-CV-01155-EJD, 2024 WL 333893, at *16 (N.D. Cal. Jan. 29, 2024) (dismissing plaintiffs' intrusion upon seclusion claim where complaint failed to allege that defendant "intentionally intruded" or that the intrusion was highly offensive). As a matter of law, the undisputed facts cannot make out the intent element of the privacy torts.

Because Plaintiffs cannot establish any of the elements of their privacy claims, summary judgment should be granted in Google's favor on those claims.

C. Plaintiffs cannot establish harm for any of their claims.

Harm is a necessary element of the intentional torts and Plaintiffs' CDAFA claim, and Plaintiffs cannot show any harm to the class as a result of Google's conduct. *See Perkins v. LinkedIn Corp.,* 53 F. Supp. 3d 1190, 1219 (N.D. Cal. 2014) (dismissing plaintiffs' CDAFA claims on the basis that Plaintiffs did not adequately allege that they had suffered any "tangible harm from the alleged Section 502 violations~~.");~~"); *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1090 (N.D. Cal. 2022) ("Determining whether a defendant's actions were 'highly offensive to a reasonable person' requires a 'holistic consideration of factors such as the ***likelihood of serious harm*** to the victim, the degree and setting of the intrusion, the ~~intruder's~~intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive.'") (quoting *Facebook Tracking*, 956 F.3d at 606 (quoting *Hernandez~~,~~ v. Hillsides, Inc.*, 211 P.3d ~~at~~1063, 1073 (2009)) (emphasis added).

Google opposed class certification in part on the basis of individualized harm inquiries. The Court rejected that argument and accepted that Plaintiffs could demonstrate class-wide harm, reasoning that "even if Google is right, and the 'vast majority' of class members' data was only exposed to record-keeping 'not tied to a person's identity or used by Google for any purpose other than to perform accounting for the apps that generated the data or advertising in the first place,' Opp~~.~~., at 16, then surely that can be proven by common evidence of Google's record-keeping practices." ECF No. 352, at 12. Plaintiffs' certified class thus must proceed on a theory that the money Google made by keeping receipts for the advertising it sold is the appropriate measure of class-wide damages, regardless of whether keeping receipts harmed any individual class member.

The problem with this theory is that Google's conduct cannot be said to have harmed any class member in particular or the class at large, because its conduct did not exploit any class member's privacy, did not intrude upon their private space, or take from them something they intended to keep for themselves or sell to another, *i.e.*, pseudonymous data about their use of Firebase-enabled apps. No court has ever found that such basic record-keeping is harmful to anyone.

To fix this problem, Plaintiffs have previously relied on an entitlement to disgorgement of profits to allege harm under their tort and CDAFA claims, based on a single sentence in the Ninth Circuit's decision in *Facebook Internet Tracking*, 956 F.3d 589. But, as Judge Chhabria has pointed out, the court's analysis on this was solely focused on Article III standing, not the damage or harm required to establish liability under Plaintiffs' tort and CDAFA claims. *See McClung,* 2024 WL 189006, at *2. ("The Court continues to be skeptical of the ~~plaintiffs'~~plaintiffs' theory that ~~California's~~California's statutory standing requirement for these claims can be satisfied simply by alleging that the defendant was unjustly enriched by the misappropriation of personal information."). Further, "the Article III analysis in that section of *Facebook Internet Tracking* has been superseded by *TransUnion*, making it even more of a stretch to rely on that section as an implicit statement about statutory standing under California law. *Id.* at n.2 (citing *TransUnion*, 594 U.S. at 426~~–~~–30).

Finally, to the extent Plaintiffs seek to rely on the subjective experiences of the Named Plaintiffs, that would belie the theory of damages Plaintiffs pushed in order to certify the class. They

cannot now backtrack and argue that the idiosyncratic emotional experiences of 100 million class members can be proven class-wide; obviously they cannot be. In other words, Plaintiffs argued themselves into a corner: they cannot tell this Court that they need not prove actual damages in order to certify a class, only to argue now in opposition to summary judgment that they can prove actual class-wide harm using common proof. The two are irreconcilable.

D. Plaintiffs' analysis of the CDAFA claim's "without permission" requirement focuses on the wrong permission-giver.

Plaintiffs' CDAFA claim fails for the reasons discussed above. But the CDAFA claim fails for the additional reason that Plaintiffs cannot establish that Google acted "without permission," even if app developers' end users failed to consent to their use of ~~GA for Firebase~~GA4F by virtue of their (s)WAA settings, because the most correct lens to view this claim through is one that focuses on Google's permission vis-à-vis the app developers, not the end users.

Google never exceeded the scope of its permission to use the data gathered by app developers and sent to Google via ~~GA for Firebase~~GA4F because it is undisputed that (1) Google required app developers to obtain consent from end users for their use of ~~GA for Firebase~~GA4F (*See* Google's Resps. to Plaintiffs' Interrog., Set Six, ECF No. 364-22, at 10:25~~-~~11:18 (Appx. A-22)) and (2) Plaintiffs do *not* allege an invasion of their privacy solely by virtue of Google's function as *data processor* for app developers as their agent. Nor could they: Courts in this district have already held that when a tech company acts as a vendor for another, its scope of consent is coterminous with the party to the communication. *See Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021); *Williams v. What If Holdings, LLC*, No. C. 22-03780 WHA, 2022 WL 17869275, at *3 (N.D. Cal. Dec. 22, 2022~~). *See*~~); *see also Byars v. Hot Topic, Inc.*, 656 F. Supp. 3d 1051, 1067~~-~~68 (C.D. Cal. 2023); *Johnson v. Blue Nile, Inc.*, No. 20-cv-08183-LB, 2021 WL 1312771, at *1 (N.D. Cal. Apr. 8, 2021); *Yale v. Clicktale, Inc.*, No. 20-cv-07575-LB, 2021 WL 1428400, at *3 (N.D. Cal. Apr. 15, 2021).

Here, none of Google's conduct falls outside the scope of its role as vendor for the app developers. Google does not make copies of the (s)WAA-off data for itself to, e.g., enhance its marketing profiles or better personalize advertising. It does not sell or exploit the data. It processes

the data sent to it under contracts with third party entities who collected it. And those contracts permit Google to use the data for various uses. Plaintiffs have never alleged that Google exceeded that scope of permission, so no CDAFA claim could lie.

VI. CONCLUSION

For the foregoing reasons, the Court should dismiss this case with prejudice.

Dated: April 4~~March 28~~, 2024

Respectfully submitted,

WILLKIE FARR & GALLAGHER LLP

By: */s/ Eduardo E. Santacana*

Benedict Y. Hur
Simona Agnolucci
Eduardo E. Santacana
Argemira Flórez
Harris Mateen

Attorneys for Defendant Google LLC